Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive

D1.2: National profiles deliverable (WP1)

National Country Profiles

---

European Commission
Internal Market Directorate-General

Brussels
SUMMARY:
The eDocuments Study Team, consisting of Siemens IT Solutions and Services and time.lex, have been contracted by the European Commission – DG Markt to perform the Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive (‘the Study’), focusing specifically on the availability, use and delivery of electronic documents in the context of article 8 of the Services Directive.

From a practical perspective, this article requires Member States to implement electronic points of single contact where service providers covered by the Directive, both national and from other Member States, can electronically complete all procedures and formalities in order to be allowed to start or exercise a service activity in that country (including by submitting and receiving e.g. extracts from the commercial register, extracts from professional registers, criminal records, statements from the service providers, certificates of insurance, proof of qualifications (such as diplomas), etc.).

This first report describes the availability and use of electronic documents in the Member States and EEA countries, focusing specifically on the context of the Services Directive. This report will be the first input for further analysis in the eDocuments Study, which should ultimately allow the Study Team to formulate recommendations on how the Commission can assist the countries in improving the interoperability and usability of electronic documents and electronic delivery.

KEYWORDS:

Services Directive
Point of Single Contact
Electronic documents
Electronic Signatures
## Document Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Issue Date</th>
<th>Description</th>
<th>Modified paragraphs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>19-Dec-08</td>
<td>First version – Germany and Portugal to be updated.</td>
<td>All sections</td>
</tr>
<tr>
<td>1.1</td>
<td>23-Dec-08</td>
<td>German profile updated; Portugal to be updated.</td>
<td>German profile</td>
</tr>
<tr>
<td>1.2</td>
<td>16-Jan-09</td>
<td>Minor updates following comments from national experts</td>
<td>German profile, French profile</td>
</tr>
<tr>
<td>1.3</td>
<td>24-Feb-09</td>
<td>Minor updates following further review by national experts</td>
<td>Cypriot, Italian, Danish, French and Romanian profiles</td>
</tr>
</tbody>
</table>
Contacts

<table>
<thead>
<tr>
<th>Code</th>
<th>Name</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Graux, Hans</td>
<td>+32 479 79 55 00</td>
<td><a href="mailto:hans.graux@timelex.eu">hans.graux@timelex.eu</a></td>
</tr>
</tbody>
</table>
Table of Contents

1 DOCUMENTS 3
   1.1 APPLICABLE DOCUMENTS 3
   1.2 REFERENCE DOCUMENTS 3

2 GLOSSARY 3

3 INTRODUCTION 3
   3.1 SCOPE AND OBJECTIVES OF THE PROJECT 3
   3.2 STRUCTURE OF THE PROJECT 3
   3.3 GOAL OF THIS DOCUMENT 3
   3.4 CREDITS AND CONTRIBUTORS 3

4 AUSTRIA 3
   4.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
   4.2 SPECIFIC DOCUMENT TYPES 3
   4.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT 3
   4.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

5 BELGIUM 3
   5.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
   5.2 SPECIFIC DOCUMENT TYPES 3
   5.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT 3
   5.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

6 BULGARIA 3
   6.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
   6.2 SPECIFIC DOCUMENT TYPES 3
   6.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT 3
   6.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

7 CYPRUS 3
   7.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
   7.2 SPECIFIC DOCUMENT TYPES 3
7.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

7.4 Assessment – plans, progress and proposals for further harmonisation

8 Czech Republic

8.1 General framework for electronic documents in eGovernment applications

8.2 Specific document types

8.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

8.4 Assessment – plans, progress and proposals for further harmonisation

9 Denmark

9.1 General framework for electronic documents in eGovernment applications

9.2 Specific document types

9.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

9.4 Assessment – plans, progress and proposals for further harmonisation

10 Estonia

10.1 General framework for electronic documents in eGovernment applications

10.2 Specific document types

10.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

10.4 Assessment – plans, progress and proposals for further harmonisation

11 Finland

11.1 General framework for electronic documents in eGovernment applications

11.2 Specific document types

11.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

11.4 Assessment – plans, progress and proposals for further harmonisation

12 France

12.1 General framework for electronic documents in eGovernment applications

12.2 Specific document types

12.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

12.4 Assessment – plans, progress and proposals for further harmonisation

13 Germany
13.1 General Framework for Electronic Documents in eGovernment Applications

13.2 Specific Document Types

13.3 Delivering Electronic Documents to Service Providers in the Context of the Point of Single Contact

13.4 Assessment – Plans, Progress and Proposals for Further Harmonisation

14 Greece

14.1 General Framework for Electronic Documents in eGovernment Applications

14.2 Specific Document Types

14.3 Delivering Electronic Documents to Service Providers in the Context of the Point of Single Contact

14.4 Assessment – Plans, Progress and Proposals for Further Harmonisation

15 Hungary

15.1 General Framework for Electronic Documents in eGovernment Applications

15.2 Specific Document Types

15.3 Delivering Electronic Documents to Service Providers in the Context of the Point of Single Contact

15.4 Assessment – Plans, Progress and Proposals for Further Harmonisation

16 Iceland

16.1 General Framework for Electronic Documents in eGovernment Applications

16.2 Specific Document Types

16.3 Delivering Electronic Documents to Service Providers in the Context of the Point of Single Contact

16.4 Assessment – Plans, Progress and Proposals for Further Harmonisation

17 Ireland

17.1 General Framework for Electronic Documents in eGovernment Applications

17.2 Specific Document Types

17.3 Delivering Electronic Documents to Service Providers in the Context of the Point of Single Contact

17.4 Assessment – Plans, Progress and Proposals for Further Harmonisation

18 Italy

18.1 General Framework for Electronic Documents in eGovernment Applications

18.2 Specific Document Types

18.3 Delivering Electronic Documents to Service Providers in the Context of the Point of Single Contact
18.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

19 LATVIA 3
19.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
19.2 SPECIFIC DOCUMENT TYPES 3
19.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT 3
19.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

20 LIECHTENSTEIN 3
20.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
20.2 SPECIFIC DOCUMENT TYPES 3
20.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT 3
20.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

21 LITHUANIA 3
21.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
21.2 SPECIFIC DOCUMENT TYPES 3
21.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT 3
21.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

22 LUXEMBOURG 3
22.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
22.2 SPECIFIC DOCUMENT TYPES 3
22.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT 3
22.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

23 MALTA 3
23.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
23.2 SPECIFIC DOCUMENT TYPES 3
23.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT 3
23.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION 3

24 THE NETHERLANDS 3
24.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS 3
24.2 SPECIFIC DOCUMENT TYPES

24.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICES PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT

24.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATIONS

25 NORWAY

25.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS

25.2 SPECIFIC DOCUMENT TYPES

25.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT

25.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION

26 POLAND

26.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS

26.2 SPECIFIC DOCUMENT TYPES

26.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT

26.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION

27 PORTUGAL

27.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS

THE MAIN AIMS OF CASA PRONTA (FAST-TRACK HOME BUYING SCHEME) ARE:

27.2 SPECIFIC DOCUMENT TYPES

27.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT

27.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION

28 ROMANIA

28.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS

28.2 SPECIFIC DOCUMENT TYPES

28.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT

28.4 ASSESSMENT – PLANS, PROGRESS AND PROPOSALS FOR FURTHER HARMONISATION

29 SLOVAKIA

29.1 GENERAL FRAMEWORK FOR ELECTRONIC DOCUMENTS IN eGOVERNMENT APPLICATIONS

29.2 SPECIFIC DOCUMENT TYPES

29.3 DELIVERING ELECTRONIC DOCUMENTS TO SERVICE PROVIDERS IN THE CONTEXT OF THE POINT OF SINGLE CONTACT
eDocuments and e-Delivery in the context of the services directive
Country Profiles report

29.4 **Assessment – Plans, progress and proposals for further harmonisation** 3

30 **Slovenia** 3

30.1 **General framework for electronic documents in eGovernment applications** 3

30.2 **Specific document types** 3

30.3 **Delivering electronic documents to service providers in the context of the Point of Single Contact** 3

30.4 **Assessment – Plans, progress and proposals for further harmonisation** 3

31 **Spain** 3

31.1 **General framework for electronic documents in eGovernment applications** 3

31.2 **Specific document types** 3

31.3 **Delivering electronic documents to service providers in the context of the Point of Single Contact** 3

31.4 **Assessment – Plans, progress and proposals for further harmonisation** 3

32 **Sweden** 3

32.1 **General framework for electronic documents in eGovernment applications** 3

32.2 **Specific document types** 3

32.3 **Delivering electronic documents to service providers in the context of the Point of Single Contact** 3

32.4 **Assessment – Plans, progress and proposals for further harmonisation** 3

33 **United Kingdom** 3

33.1 **General framework for electronic documents in eGovernment applications** 3

33.2 **Specific document types** 3

33.3 **Delivering electronic documents to service providers in the context of the Point of Single Contact** 3

33.4 **Assessment – Plans, progress and proposals for further harmonisation** 3
# Documents

## 1 Applicable Documents

<table>
<thead>
<tr>
<th>[AD1]</th>
<th>Framework Contract ENTR/05/58-SECURITY</th>
</tr>
</thead>
</table>

## 1.2 Reference Documents

|--------|-----------------------------------------------------------------------------------|
| [RD2] | Handbook on implementation of the Services Directive
| [RD4] | IDABC Work Programme Third Revision
2 Glossary

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and have also been used by the correspondents in their reports:

- **Service**: any self-employed economic activity, normally provided for remuneration, as referred to in Article 50 of the E.U. Treaty;

- **Service provider**: any entity (natural person, legal person or organisation without legal personality) that provides a service as defined above, thus excluding employees.

- **Electronic document or eDocument**: any document in an electronic form regardless of the specific formats or solutions used that is issued by public authorities or private bodies to the service provider, or submitted by the service provider when completing procedures and formalities necessary to establish or to carry out a service.

- **Point of Single Contact (PSC)**: organisation or entity which national and foreign service providers can address to complete all procedures and formalities relating to access to a service activity and to the exercise thereof within a country, at a distance and by electronic means, as required by article 8 of the Services Directive.

- **Requirement**: any obligation, prohibition, condition or limit provided for in the laws, regulations or administrative provisions of the Member States or in consequence of case-law, administrative practice, the rules of professional bodies, or the collective rules of professional associations or other professional organisations, adopted in the exercise of their legal autonomy; rules laid down in collective agreements negotiated by the social partners shall not as such be seen as requirements.

- **eSignature**: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- **Advanced electronic signature**: an electronic signature which meets the following requirements:
  (a) it is uniquely linked to the signatory;
  (b) it is capable of identifying the signatory;
  (c) it is created using means that the signatory can maintain under his sole control; and
  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

- **Qualified electronic signature**: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive\(^1\).

---

3 Introduction

3.1 Scope and objectives of the project

The eDocuments Study Team, consisting of Siemens IT Solutions and Services and time.lex, have been contracted by the European Commission – DG Markt to perform a study on the existing situation and plans with regard to electronic documents and electronic delivery in the Member States and EEA Countries (‘the Study’), in particular examining solutions used or planned to be used in the context of the implementation of the Services Directive. Article 8 of the Directive contains an obligation for Member States that could have a significant impact on the way they issue and accept electronic documents:

“Article 8 – Procedures by electronic means

1. Member States shall ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact and with the relevant competent authorities.

2. Paragraph 1 shall not apply to the inspection of premises on which the service is provided or of equipment used by the provider or to physical examination of the capability or of the personal integrity of the provider or of his responsible staff.

3. The Commission shall, in accordance with the procedure referred to in Article 40(2), adopt detailed rules for the implementation of paragraph 1 of this Article with a view to facilitating the interoperability of information systems and use of procedures by electronic means between Member States, taking into account common standards developed at Community level.”

From a practical perspective, this article requires Member States to implement electronic Points of Single Contact (also referenced in this document as PSCs) where service providers covered by the Directive, both national and from other Member States, can electronically complete all procedures and formalities in order to be allowed to start or exercise a service activity in that country, including by submitting and receiving specific documents, such as extracts from the commercial register, extracts from professional registers, criminal records, statements from the service providers, certificates of insurance, proof of qualifications (such as diplomas), etc. This Study aims to examine if and how the Member States are currently using and/or planning to use such electronic documents, specifically taking into account the scope of the Services Directive, which includes cross border situations.

The electronic interaction between the service provider and the Point of Single Contact covers the electronic exchange of documents in two directions. Service providers may be required to provide certain documentation electronically when necessary for the completion of the electronic procedure, and the competent authority may have to deliver the reply to the service provider through the Point of Single Contact.

The Commission would like to get an overview of the current situation in the Member States and EEA Countries with regard to the exchange of electronic documents between service providers and points of single contact and the electronic delivery of documents issued by public authorities, including delivery in cross-border situations.
The goal of this Study is to determine both from a technical and legal perspective how the Member States and EEA Countries:

- Are currently issuing authentic electronic documents of both public and private bodies, or are planning to issue them for the purposes of Art.8 of the Directive, and what technical solutions are used;
- Are currently accepting electronic documents from other Member States, and which requirements apply in this case, in particular with regard to rules of format and means for authentication;
- Are already electronically delivering documents issued by public administrations or private bodies, or are planning to put delivery systems in place when setting up their points of single contact, including cross-border delivery and technical solutions involved.

At the end of the Study, this should allow the Study Team to formulate recommendations on how the Commission can assist the countries in improving the interoperability and usability of electronic documents and electronic delivery.

### 3.2 Structure of the project

The Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive consists of 3 different phases.

- In the first phase (Work Package 1), information is collected on the current status of the implementation of article 8 of the Services Directive in the Member States, focusing both on the general strategy for issuing and accepting electronic documents, and on solutions which are available or envisaged for a number of specific document types, as will be explained below. The main goal of this first phase is to get a representative overview of the kinds of electronic documents which are currently already in use in the Member States, and which documents the Member States are planning to use, especially in the context of Points of Single Contact, and keeping into account the cross border dimension.

- In the second phase (Work Package 2), the collected information will be analysed in order to determine any similarities and differences in the national approaches to the implementation of article 8 or to the treatment of electronic documents in general, and to assess the impact of the choices made (or not yet made) by the Member States on the accessibility of the services to foreign service providers. This includes specifically the identification of mitigation strategies to reduce the interoperability difficulties in the Member States.

- Finally, in the third phase (Work Package 3), specific recommendations will be provided in order to realise the best feasible level of interoperability and/or exchangeability of electronic documents by the end of 2009, and addressing the major issues identified in WP 2, including by proposing any necessary steps to be taken at the E.U. level to achieve the described level of interoperability.
3.3 Goal of this document

This document ("Country profiles report") concerns the first phase outlined above: it will provide a description of the types of electronic documents currently being issued to service providers and currently being accepted by public administrations, both from a technical and legal perspective. The Member States’ efforts to implement the Services Directive will take a central role in this regard, as the operation of a functioning Point of Single Contact will likely require service providers to be able to submit documents in an electronic format to the PSC, and to receive such documents from the PSC, at least in some countries.

As a first step in this Study, the eServices Study Team has identified the existing situation at the national level. For each Member State and EEA Country, information was collected on:

- The question of whether electronic documents are currently already being used in electronic procedures, and if so, in what form. This includes the legal framework applicable to such documents, the technical standards that are adhered to as well as formats, the structure requested and the readiness for automated processing and recognition of content.

- How the national administrations are planning to integrate electronic documents into their Point(s) of Single Contact. This includes two aspects:
  
  o First of all, how will service providers be able to provide electronic documents to the Point(s) of Single Contact? What legal or technical framework exists at a horizontal (incl. regional and local) level setting out the requirements for authentic e-documents in general or for those issued by public authorities or private bodies, as well as the requirements for the acceptance by the competent authorities of authentic electronic documents. What kind of structure is requested for a concrete document (on the basis of examples listed above), and is the automated processing and recognition of specific information (such as name, profession, etc) possible?

  o Secondly, how will electronic documents issued by public authorities or private bodies be delivered to the service provider by the Point(s) of Single Contact? Has a legal or technical framework been put in place or is it under consideration yet, including for cross-border delivery? Will the technical solution involved to implement the delivery be deployed uniformly at the national level or is the choice of electronic delivery and possible solutions left to the individual authority?

With regard to specific electronic documents, the reports below describe both the general strategy adopted in each country with regard to the use of electronic documents in a public sector documents, and more detailed information for certain specific document types likely to be commonly encountered in the context of a Point of Single Contact, most notably extracts from the commercial register, extracts from professional registers, criminal records, statements from service providers, certificates of insurance, proof of qualifications (diplomas etc) requested from service providers for completion of relevant procedures and formalities.
This information has been collected through a network of national experts, who have assisted the Study Team in drafting a national profile for their country as will be further described below.
### 3.4 Credits and contributors

Reports such as these are only possible through the assistance of local experts who are capable and willing of providing information with regard to their legal frameworks and administrative practices. The Study team especially wants to acknowledge the contributions of the following authors for each of the country profiles:

<table>
<thead>
<tr>
<th>E.U. Member States</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Max W. Mosing, attorney-at-law at Gassauer Fleissner attorneys-at-law</td>
</tr>
<tr>
<td></td>
<td>(<a href="mailto:m.mosing@gassauer.at">m.mosing@gassauer.at</a>; <a href="http://www.gassauer.at">www.gassauer.at</a>)</td>
</tr>
<tr>
<td>Belgium</td>
<td>Hans Graux (time.lex Law Offices – <a href="http://www.timelex.eu">www.timelex.eu</a>)</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Dr. George Dimitrov, Dimitrov, Petrov &amp; Co. Law Firm (<a href="http://www.dpc.bg">www.dpc.bg</a>)</td>
</tr>
<tr>
<td></td>
<td>Ms. Desislava Krusteva, Dimitrov, Petrov &amp; Co. Law Firm (<a href="http://www.dpc.bg">www.dpc.bg</a>)</td>
</tr>
<tr>
<td>Cyprus</td>
<td>Olga Georgiades (Lexact Business &amp; Legal Solutions)</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Tomas Schollaert (Pierstone Law Offices)</td>
</tr>
<tr>
<td>Denmark</td>
<td>Jan Trzaskowski, Law Department of Copenhagen Business School,</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cbs.dk/law">www.cbs.dk/law</a></td>
</tr>
<tr>
<td>Estonia</td>
<td>Kaupo Lepasepp, Sorainen law firm (<a href="http://www.sorainen.ee">www.sorainen.ee</a>)</td>
</tr>
<tr>
<td></td>
<td>Mihkel Milda, Sorainen law firm (<a href="http://www.sorainen.ee">www.sorainen.ee</a>)</td>
</tr>
<tr>
<td>Finland</td>
<td>Teemu Rissanen, Conseils Oy (<a href="http://www.conseils.fi">www.conseils.fi</a>)</td>
</tr>
<tr>
<td>France</td>
<td>Fanny Coudert (time.lex Law Offices – <a href="http://www.timelex.eu">www.timelex.eu</a>)</td>
</tr>
<tr>
<td>Germany</td>
<td>Gerald Spindler, Professor, Law School, University of Goettingen (<a href="http://www.gerald-spindler.de">www.gerald-spindler.de</a>)</td>
</tr>
<tr>
<td>Greece</td>
<td>Eleni Kosta, time.lex law firm (<a href="http://www.timelex.eu">www.timelex.eu</a>)</td>
</tr>
<tr>
<td>Hungary</td>
<td>M. András Gerencsér, (<a href="mailto:gerencser@enternet.hu">gerencser@enternet.hu</a>)</td>
</tr>
<tr>
<td>Ireland</td>
<td>Professor Maeve McDonagh &amp; Ms. Fidelma White (University College Cork)</td>
</tr>
<tr>
<td>Italy</td>
<td>Davide Maria Parrilli, Interdisciplinary Centre for Law and ICT – ICRI, Catholic University of Leuven, IBBT – <a href="http://www.icri.be">www.icri.be</a></td>
</tr>
<tr>
<td>Latvia</td>
<td>Kaspars Fridenbergs-Ansbergs and Agis Repšs, Sorainen (<a href="http://www.sorainen.lv">www.sorainen.lv</a>)</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Erika Budaitė and Renata Beržanskiienė, Sorainen Law Firm (<a href="http://www.sorainen.lt">www.sorainen.lt</a>)</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Laurent Fisch, partner and Claire Leonelli, associate - Molitor, Fisch &amp; Associates law firm (<a href="http://www.mfa.lu">www.mfa.lu</a>)</td>
</tr>
<tr>
<td>Malta</td>
<td>Paul Gonzi, Fenech &amp; Fenech law firm (<a href="http://www.fenechlaw.com">www.fenechlaw.com</a>)</td>
</tr>
<tr>
<td></td>
<td>Antonio Ghio, Fenech &amp; Fenech law firm (<a href="http://www.fenechlaw.com">www.fenechlaw.com</a>)</td>
</tr>
<tr>
<td>Poland</td>
<td>Dr. Dariusz Adamski, The Research Centre for Legal and Economic Issues of Electronic Communication (cbke.prawo.uni.wroc.pl)</td>
</tr>
<tr>
<td>Portugal</td>
<td>Pedro Simões Dias, Fujitsu Services Head of Commercial and Legal</td>
</tr>
<tr>
<td>Romania</td>
<td>Corina Papuzu, Petru Buzescu Law Firm (<a href="http://www.buzescu.com">www.buzescu.com</a>)</td>
</tr>
<tr>
<td>Slovakia</td>
<td>Zuzana Mikulášková, National Security Authority (<a href="http://www.nbusr.sk">www.nbusr.sk</a>)</td>
</tr>
<tr>
<td>Slovenia</td>
<td>Klemen Tičar, Ulčar-op d.n.o., law firm</td>
</tr>
<tr>
<td>Spain</td>
<td>Cristina de Lorenzo, Sánchez Pintado &amp; Núñez, Abogados, law firm (<a href="http://www.span-n.com">www.span-n.com</a>)</td>
</tr>
<tr>
<td>Sweden</td>
<td>Christine Kirchberger, Swedish Law and Informatics Research Institute</td>
</tr>
<tr>
<td></td>
<td>(<a href="http://www.juridicum.su.se">www.juridicum.su.se</a>)</td>
</tr>
</tbody>
</table>
eDocuments and e-Delivery
in the context of the services directive
Country Profiles report

<table>
<thead>
<tr>
<th>Country</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Netherlands</td>
<td>A.H. Ekker and L.H.M. Eijpe Skoop advocaten (<a href="http://www.skoopadvocaten.nl">www.skoopadvocaten.nl</a>)</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Prof. Ian Lloyd (Professor of Information Technology Law, University of Strathclyde)</td>
</tr>
</tbody>
</table>

**E.E.A. Countries**

<table>
<thead>
<tr>
<th>Country</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iceland</td>
<td>Haraldur Bjarnason, Ministry of Finance</td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>Norbert Ospelt, Amt für Personal und Organisation (APO), Liechtenstein</td>
</tr>
<tr>
<td>Norway</td>
<td>Thomas Myhr, Ministry of Trade and Industry (<a href="http://www.nhd.no">www.nhd.no</a>)</td>
</tr>
</tbody>
</table>

In addition, their efforts were validated by local officials and experts involved in the implementation of the Services Directive in their respective countries, including most notably the following. It should be noted however that the reports themselves were drafted by the aforementioned authors, and that responsibility for any errors or omissions lies with the authors.

**E.U. Member States**

<table>
<thead>
<tr>
<th>Country</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Peter Kustor, Head eGov Unit, Federal Chancellery, <a href="mailto:peter.kustor@bka.gv.at">peter.kustor@bka.gv.at</a></td>
</tr>
<tr>
<td>Belgium</td>
<td>M. Luc Gathy, Agence pour la Simplification Administrative, SPF Chancellerie du Premier Ministre; <a href="http://www.simplification.fgov.be/">www.simplification.fgov.be</a> and M. Frank Leyman, Manager International Relations Fedict – Federal Public Service ICT; <a href="http://www.fedict.be">www.fedict.be</a></td>
</tr>
<tr>
<td>Cyprus</td>
<td>Mrs Aliki Serghi, Planning Bureau</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Michal Roubik, <a href="mailto:roubik@mpo.cz">roubik@mpo.cz</a></td>
</tr>
<tr>
<td>Denmark</td>
<td>Thor Iversen, Danish Enterprise and Construction Authority, <a href="http://www.deaca.dk">www.deaca.dk</a>, <a href="mailto:ti@ebst.dk">ti@ebst.dk</a> Charlotte Jacoby, National IT and Telecom Agency, <a href="http://www.itst.dk">www.itst.dk</a>, <a href="mailto:cj@itst.dk">cj@itst.dk</a></td>
</tr>
<tr>
<td>Estonia</td>
<td>Uuno Vallner, Ministry of Economic Affairs and Communications, Department of State Information Systems (RISO), Head of the IT Infrastructure Division, <a href="http://www.riso.ee">www.riso.ee</a></td>
</tr>
<tr>
<td>Finland</td>
<td>M. Olli-Pekka Rissanen, Ministry of Finance; <a href="http://www.valtit.fi">www.valtit.fi</a> M. Mikko Holm, Ministry of Labour and the Economy; <a href="http://www.tem.fi">www.tem.fi</a></td>
</tr>
<tr>
<td>France</td>
<td>Ms. Marie José Palasz, Chef de mission, Mission “Transposition de la directive services”, CGEFi</td>
</tr>
<tr>
<td>Germany</td>
<td>Dr. Harald Neymanns, Bundesministerium des Innern (<a href="http://www.bmi.bund.de">www.bmi.bund.de</a>)</td>
</tr>
<tr>
<td>Greece</td>
<td>Dr. Antonios Stasis, Greek Ministry of Interior, General Secretariat of Public Administration and eGovernment.</td>
</tr>
<tr>
<td>Hungary</td>
<td>Mr. József Buzder Lantos, Prime Minister’s Office, Department of e-Administration, State Secretariat for ICT &amp; e-Government; <a href="http://www.ekk.gov.hu/en">http://www.ekk.gov.hu/en</a></td>
</tr>
<tr>
<td>Ireland</td>
<td>Michael Clarke and Sean Smith, Department of Enterprise Trade and Employment Claire Pyke, Companies Registration Office Supt. Pat Burke, An Garda Síochána Ann McNicholl, Royal Institute of Architects of Ireland Denis McGrath and Deborah O’Sullivan, Engineers Ireland</td>
</tr>
<tr>
<td>Country</td>
<td>Author(s)</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Italy</td>
<td>Angela Manley, Registrar’s Office, University College Cork</td>
</tr>
<tr>
<td>Latvia</td>
<td>Ms. Inese Betaka, Head of International Policy Unit, Minister for Electronic Government Affairs</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Ms. Inga Petravičiūtė, Head of the e-Documents Division, Lithuanian Archives Department (<a href="http://www.archyvai.lt">www.archyvai.lt</a>)</td>
</tr>
<tr>
<td>Luxemburg</td>
<td>M. Ricky Wohl, conseiller de direction du Service eLuxembourg (ministère de la Fonction publique et de la Réforme administrative)</td>
</tr>
<tr>
<td>Malta</td>
<td>Mr Derrick Pisani (MITTS Ltd.)</td>
</tr>
<tr>
<td>Poland</td>
<td>M. Marcin Fijałkowski, Ministerstwo Gospodarki; <a href="http://www.mg.gov.pl">www.mg.gov.pl</a></td>
</tr>
<tr>
<td>Portugal</td>
<td>Angelo Seiça Neves (Ministério da Economia e da Inovação)</td>
</tr>
<tr>
<td>Slovakia</td>
<td>Juraj Paluš, Ministry of Justice (<a href="http://www.justice.gov.sk">www.justice.gov.sk</a>)</td>
</tr>
<tr>
<td>Slovenia</td>
<td>Mr. Dušan Žužič, Ministry of the economy</td>
</tr>
<tr>
<td>Spain</td>
<td>Mª Montaña Merchán Arribas, <a href="mailto:mmontana@map.es">mmontana@map.es</a></td>
</tr>
<tr>
<td>Sweden</td>
<td>Clas Heinegard, Swedish Ministry for Foreign Affairs</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Craig Belshaw of the Department for Business, Enterprise and Regulatory Reform.</td>
</tr>
</tbody>
</table>

**E.E.A. Countries**

<table>
<thead>
<tr>
<th>Country</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iceland</td>
<td>Halla-Bjorg Baldursdottir, Prime Minister’s Office</td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>Norbert Ospelt, Amt für Personal und Organisation (APO), Liechtenstein</td>
</tr>
<tr>
<td>Norway</td>
<td>Mr. Pål Somdalen, Ministry of Trade and Industry (<a href="http://www.nhd.no">www.nhd.no</a>)</td>
</tr>
<tr>
<td></td>
<td>Mr. Sverre Hovland, Brønnøysund Register Center (<a href="http://www.brreg.no">www.brreg.no</a>)</td>
</tr>
</tbody>
</table>

The eDocuments Study team wishes to express its gratitude towards all authors and contributors to this report.
4 Austria

4.1 General framework for electronic documents in eGovernment applications

4.1.1 Electronic documents in eGovernment applications

Austrian eGovernment Applications and the Austrian e-Government Act

During the eGovernment Conference of Ministers in Lisbon on 20 September 2007, Austria was declared the European champion in eGovernment for the second time in a row. The online sophistication of base services in Austria is measured at 99% and all services were graded level 4 or 5. This means that, according to the indicator, 100% of online capability has been achieved.²

The use of Electronic Documents in Austrian eGovernment Applications is based on a scheme of (a) identification and (b) validation/authentication/integrity: Austria implemented a “Federal Act on Provisions Facilitating Electronic Communications with Public Bodies - Austrian E-Government Act”³ (E-Government-Gesetz) in 2004. The object of the Austrian E-Government Act is to promote legally relevant electronic communication between public bodies and so called Data Subjects (Betroffener)⁴. Electronic communications with public bodies are to be facilitated, having regard to the principle of freedom to choose between different means of communication when making submissions to such bodies.

The Austrian E-Government Act addresses specifically the electronic validation of data, namely (i) information on economic activity as a self-employed person, (ii) data concerning personal status and nationality and (iii) other data (details see below). Furthermore, the peculiarities of keeping electronic records are regulated by the Austrian E-Government Act (details see below).

The Austrian E-Government Act also deals with the issue of the improvement of legal protection in the context of electronic communication between public bodies and Data Subjects: Specific technical means shall be created to counter the risks associated with an increased use of automated data processing for the purposes of achieving the aims set out above and implemented where other precautions do not already provide adequate protection – however, the Austrian E-Government Act

² [URL]


⁴ Pursuant to Sec 2 No 7 Austrian E-Government Act "Data Subject" is any natural or legal person or other association or institution having its own identity for the purposes of legal or economic relations.
does not specify the concrete technical measures, but lays down the named guidelines; this has the advantage that otherwise technical measures could become outdated, which is avoided by not referring to concrete measures.

Furthermore, with respect to implementation of the aims of the Austrian E-Government Act, measures shall be taken to ensure that official Internet sites which provide information or electronic support for procedures are structured in such a way as to comply with international standards for access to the world wide web, including unhindered access for disabled persons. Again, the Austrian E-Government Act does not refer to concrete technical measures.

Therefore, the Austrian E-Government Act sets out the framework regarding the eGovernment application. However, the Austrian E-Government Act does not stipulate the entire regulations for eGovernment applications, but “only” sets out the general framework.

Citizen Card for (a) identification and (b) validation/authentication/integrity

One major issue of eGovernment application generally is the identity and authenticity of the acts and Electronic Documents in such applications. The Austrian E-Government Act stipulates that the base for the identity and authenticity in eGovernment applications is the so called “Citizen Card” (Bürgerkarte – see [link to Bürgerkarte website]). The Citizen Card is a logical unit that, independent of its technical implementation combines a Qualified Electronic Signature (Qualifizierte Elektronische Signatur) with an Identity Link (Personenbindung) and the associated security data and functions as well as any existing data on representation; see for technical specification of the Citizen Card scheme: [link to Citizen Card scheme website].

The user needs the following infrastructure for using the Citizen Card scheme: (i) a computer with Internet access; (ii) a card reader, a built-in device or keyboard or an external reader; (iii) a compatible chip card that can be used as a citizen card, such as electronic social insurance card (e-card – see also below), Signature Card, bank cards (eg Maestro), student cards (Studentenausweis), identification cards from government ministries (Dienstausweise), other official cards (for example, a notary’s card (Notarsausweis) or attorney-at-law’s card (Rechtsansaltausweis)) (iv) a software program that supports the Citizen Card scheme: The Federal Chancellery (Bundeskanzleramt) offers

5 Definition of a Qualified Electronic Signature: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

6 Sec 2 No 10 Austrian E-Government Act.

7 [link to Citizen Card infrastructure website].

8 Where to get: [link to Citizen Card infrastructure website].

9 See details: [link to Citizen Card infrastructure website].

10 [link to Citizen Card infrastructure website].
Citizen Card software free-of-charge (IT solution trustDesk basic\textsuperscript{11}). Other free software programs are BDC HotSign\textsuperscript{12} and the a-sign client\textsuperscript{13}. This middleware, the so called Citizen Card Environment (Bürgerkartenumgebung), provides a high-level abstraction layer. Applications use this middleware to make use of the Citizen Card’s functions. Current Citizen Card Environment implementations have to be installed on the user’s PC. This has the significant drawback that the user must install a piece of software before he can use a Citizen Card enabled application. To overcome this situation, an “Online Citizen Card Environment” has been released most recently. It is based on zero-footprint-technology: only the minimum piece of software, required to access the user’s Citizen Card, runs on the client’s machine. To execute this software from the browser it is implemented as Java applet. (see for instance the option “Online CCS” at: \url{https://www.buergerkarte.at/pdf-as/?locale=en}).

From electronic social insurance card (e-card) to Citizen Card in just 4 steps:\textsuperscript{14} 1. Step: the above named infrastructure is needed; 2. Step: online activation is necessary: (a) as a registered user with tax declaration online (\url{FinanzOnline})\textsuperscript{15}, the e-card can directly be activated on the FinanzOnline website (in this case step 3 and 4 are no longer necessary); alternatively, the e-card activation web page\textsuperscript{16} can be visited and continued with step 3; 3. Step: the activation code is sent to the user by certified mail with delivery confirmation (RSa-Brief) to registered home address; 4. Step: Completing online activation by entering activation code on e-card activation web page\textsuperscript{17}.

Furthermore, it is possible to activate the e-card with Registration Officers in many entities all over Austria.\textsuperscript{18}

The Citizen Card serves to validate the unique identity of a person (Data Subject) making a submission and of the authenticity of a submission made electronically in eGovernment applications. The unique identification of a natural person who is the lawful holder of a Citizen Card shall be effected in that person’s Citizen Card by way of an Identity Link:\textsuperscript{19} the “sourcePIN Register Authority” (Stammzahlenregister) (see details below) confirms, by electronic signature, that the natural person identified in the Citizen Card as the holder has been allocated a particular source identification number (sourcePIN (Stammzahl) – see details below) for the purpose of unique identification. The Austrian E-Government Act also stipulates rules with respect to validation of identity in the event of representation (see details below). The Identity Link shall be entered in the Citizen Card by the sourcePIN Register Authority or, on its behalf, by other authorities.\textsuperscript{20}

\textsuperscript{11} \url{http://www.buergerkarte.at/en/voraussetzungen/software.html#download}.
\textsuperscript{12} \url{http://www.bdc.at}.
\textsuperscript{13} \url{http://www.a-trust.at}.
\textsuperscript{14} \url{http://www.buergerkarte.at/en/aktivieren/online.html}.
\textsuperscript{15} \url{https://finanzonline.bmf.gv.at/}.
\textsuperscript{16} \url{https://www.a-trust.at/e-card}.
\textsuperscript{17} \url{https://www.a-trust.at/e-card}.
\textsuperscript{18} \url{https://www.a-trust.at/e-card/rafinder.aspx}.
\textsuperscript{19} Sec 4 para 1 Austrian E-Government Act.
\textsuperscript{20} Sec 4 para 2 Austrian E-Government Act.
The authenticity of a submission made using the Citizen Card shall be validated by the electronic signature contained in the Citizen Card.21

Where the Citizen Card is to be used for submissions by a representative (Vertreter), a reference to the permissibility of the representation must be entered in the Citizen Card of the representative. This occurs where the sourcePIN Register Authority, having been presented with proof of an existing authority to represent or in cases of statutory representation, enters in the Citizen Card of the representative, upon application by the representative, the sourcePIN of the Data Subject and a reference to the existence of an authority to represent, including any relevant material or temporal limitations. The permission to receive documents pursuant to the Service of Documents Act (Zustellgesetz)22 must be entered separately.23 In cases of professional representation (berufsmäßige Parteienvertretung) – eg attorneys at law (Rechtsanwälte) – no particular proof of authority to represent is required if the general authority to represent is evident from the notice of professional entitlement according to the professional regulations in the signature certificate.24 Eg the attorneys-at-law’s card (Rechtsanwaltsausweis) includes a Qualified Electronic Signature and the general authority.25

Provided that such a service is offered by authorities (Behörden), officials (Organwalter) authorised especially for this purpose may, at a person's request, lodge applications for that person with all authorities, irrespective of their material and organisational competence (sachlichen und örtlichen Zuständigkeit), in procedures in which a Citizen Card may be used. The specific instruction (Auftrag) issued by the citizen shall be documented and kept by the authority in an appropriate form. Applications shall be lodged using the citizen card of the official. The general competence of an official to lodge applications for citizens must be apparent from the signature certificate in the official’s Citizen Card. In this case, the sourcePIN Register Authority shall, upon application of the official, provide the sourcePIN of the data subject directly to the citizen card enabled application where the official procedure is carried out.26

As mentioned above, the Data Subject shall be uniquely identified in the Citizen Card by his source identification number (sourcePIN). With respect to natural persons who are registered in the Central Register of Residents (CRR) (Zentrales Melderegister - ZMR)27, the source identification number shall be derived from that person's registration number in the Central Register of Residents (CRR number (ZMR-Zahl)) and secured by using strong cryptography. The source identification number of natural persons, not having to register in the CRR, shall be derived on the basis of their registration number in a Supplementary Register (Ergänzungsregister) (see below).28

21 Sec 4 para 4 Austrian E-Government Act.
23 Sec 5 para 1 Austrian E-Government Act.
24 Sec 5 para 2 Austrian E-Government Act.
27 http://zmr.bmi.gv.at.
28 Sec 6 para 2 Austrian E-Government Act.
For Data Subjects entered in the Commercial Register (Firmenbuch)\(^{29}\) the Central Register of Associations (Zentrales Vereinsregister)\(^{30}\) or the Supplementary Register (Ergänzungsregister) the sourcePIN shall be the Commercial Register Number (Firmenbuchnummer) or the Central Register of Associations number (ZVR number - Vereinsregisterzahl) or the registration number (Ordnungsnummer) allocated in the Supplementary Register (see below).\(^{31}\)

Data Subjects who are not entered in the Register of Residents and need not be entered in the Commercial Register nor in the Register of Associations shall be entered in the Supplementary Register (Ergänzungsregister) by the SourcePIN Register Authority - upon application – for the proof of their unique identity.\(^{32}\) Furthermore, Data Subjects who are not registered in the Central Register of Residents nor in the Supplementary Register may be entered in the Supplementary Register in the course of an application for the issue of a Citizen Card if the application is provided with a Qualified Electronic Signature which is linked to an equivalent electronic verification of that person’s unique identity in his or her country of origin. The Federal Chancellor shall lay down by Order further conditions for equivalence – however, such conditions have not been laid down yet and are currently discussed on European level. This will have impact on the regarding implementation of the Service Directive.

The sourcePIN Authority shall, upon application of the Data Subject, provide the SourcePIN of the Data Subject directly to the Citizen Card enabled application where the official procedure is carried out. The sourcePIN may be used by the SourcePIN Register Authority only to calculate ssPINs (bereichsspezifisches Personenkennzeichen – see below).\(^{33}\)

For the generation of source identification numbers for natural persons the sourcePIN Register Authority has to use mathematical algorithms which apply strong cryptography to the sourcePIN. These algorithms shall be determined by the sourcePIN Register Authority and - with the exception of the cryptographic key used - published on the Internet\(^{34}\).\(^{35}\)

The sourcePIN Register Authority (Stammzahlenregisterbehörde) is the Data Protection Commission,\(^{36}\) which shall perform that function by way of the Register for Data Files.\(^{37}\) The sourcePIN Register Authority (Stammzahlenregisterbehörde) has its own website (http://www.stammzahlenregister.gv.at), however, only in German, where the user can apply for

\(^{30}\) http://zvr.bmi.gv.at.
\(^{31}\) Sec 6 para 3 Austrian E-Government Act.
\(^{32}\) Sec 6 para 4 Austrian E-Government Act.
\(^{33}\) Sec 6 para 5 Austrian E-Government Act.
\(^{34}\) http://www.stammzahlenregister.gv.at/site/6001/default.aspx.
\(^{35}\) Sec 6 para 6 Austrian E-Government Act.
\(^{36}\) http://www.dsk.gv.at.
\(^{37}\) Sec 7 Austrian E-Government Act.
ssPINs (bereichspezifische Personenkennzeichen) and/or the registration of representation (Vertretungsbefugnis).

In data files of controllers in the public sector (Auftraggeber im öffentlichen Bereich), the identification of natural persons within the framework of the Citizen Card scheme may be represented only in the form of a ssPIN (bereichspezifische Personenkennzeichen - see below). With respect to persons who are not natural persons, the source identification number may be stored for the purpose of unique identification.\textsuperscript{38} The ssPIN (bereichspezifische Personenkennzeichen) is derived from the source identification number of the natural person concerned.\textsuperscript{39}

The generation of ssPINs without the use of a Citizen Card is only allowed for the sourcePIN Register Authority and is only permissible when unique identification on the basis of the ssPIN in data files of controllers in the public sector is necessary because personal data are to be processed or transmitted in conformity with the Austrian Data Protection Act (Datenschutzgesetz 2000)\textsuperscript{40}. Such cases include, in particular, administrative cooperation, data acquisition at the request of the data subject or a submission to an authority by a representative.\textsuperscript{41}

The protection of the source identification number (sourcePIN – Stammzahl) of natural persons is of importance to the concept of the Austrian E-Government Act.\textsuperscript{42} ssPINs shall not be stated in

\textsuperscript{38} Sec 8 Austrian E-Government Act.

\textsuperscript{39} The use of that derived identifier for identification purposes shall be limited to that sector of state activity which is served by the data file in which the ssPIN is to be used (Sec 9 Austrian E-Government Act). The mathematical algorithms applied to generate the ssPIN (hash function using the source identification number und the sector code) shall be determined by the sourcePIN Register Authority and published on the Internet (http://www.stammzahlenregister.gv.at/site/5972/default.aspx): The ssPIN (bereichspezifische Personenkennzeichen) is derived in two steps: (a) the sourcePIN and the sector are combined to a “Character String” (Zeichenkette); (b) with the hash function the Character String is transformed by a “secure cryptographic one-way-function” (sichere kryptografische Einwegableitung) ie a cryptographic hash function; the ssPIN is encoded by the Base64 standard (ISO-8859-1). Generally, ssPINs shall be generated by irreversible derivations from the source identification number. In the interests of the transparency of State activity, this shall not apply to ssPINs which are used exclusively in connection with the activity of a person as an official representing a public authority (Sec 13 para 1 Austrian E-Government Act).


\textsuperscript{41} Sec 10 para 2 Austrian E-Government Act.

\textsuperscript{42} Insofar as source identification numbers do not contain public data, such as the number of an entry in the Register of Company Names or the ZVR number, their confidentiality shall be subject to special protection by way of the following measures of the Citizen Card scheme: (i) The number derived from the CRR number and used as the source identification number of natural persons may be permanently stored only in the Citizen Card and only in connection with the Identity Link (Personenbindung) or in order to indicate an instance of authority to represent; (ii) source identification numbers of natural persons shall be generated in the sourcePIN Register whenever they are required. They shall not, however, be subject to storage exceeding the time necessary for generation and immediate transaction; (iii) the use of the source identification number of natural persons in order to
communications to Data Subjects or to third parties. The matching of such communications to records of the controller concerning the same subject-matter shall be facilitated by other means, such as a reference number.  

Electronic Delivery of Official Correspondence

In this context it is worth mentioning the initiative “Electronic Delivery of Official Correspondence” (Elektronische Zustellung von Erledigungen): Upon request public authorities are able to send only electronic official notifications and decisions; the Citizen Card is used to prove the identity of the sender and the recipient. The political idea behind it is: elderly people and those in the workforce will especially appreciate the fact that they no longer need to go to the post office to pick up certified mail with delivery confirmation (RSa-Briefe). The registration for this service can be done free-of-charge online at www.zustellung.gv.at; the service is available under www.meinbrief.at.

Electronic Record System (ELAK) and Official Signature

One of the most important developments of eGovernment for the Austrian Government is the Electronic Record System – ELAK (Elektronischer Akt): It enables seamless communication between public authorities and other governmental service points and shortens reaction and processing time by up to 15 percent. In 2001, the ELAK system was launched department-wide in the Austrian Ministry for Foreign Affairs and the Federal Chancellery. Since then, ELAK has been rolled out nation-wide and is also being introduced step by step in provincial governments.

The advantages of electronic record processing are obvious. ELAK substantially reduces the amount of time required for processing applications since documents no longer need to be sent back and forth between ministries and public authorities. Instead, they can be processed conveniently online. Processes are standardised and can run parallel to one another. Enquiries can be carried out directly from the desk top and the process workflow is completely transparent. With practically just a push of a button you can find out at any time of day how far the file has been processed. Furthermore, there are

43 Sec 11 Austrian E-Government Act.
never any problems due to changes in the format of the file (printed copies, scans) because ELAK is
based on a standardised system with uniform user interfaces.

To enable tele-working, an external access point allows users to connect to the electronic record
system over the Internet. With ELAK-EXT\[15\] (external), remote access to the system is available using
the Citizen Card for security.

The Austrian E-Government Act addresses also the peculiarities of keeping electronic records (in the
public sector) (elektronische Aktenführung).\[46\]

An Official Signature (Amtssignatur), being the electronic signature of a public authority, is a
Advanced Electronic Signature (elektronische Signatur) in terms of the Austrian Electronic Signature
Act (Signaturgesetz)\[47\], the peculiarity of which is indicated by an appropriate attribute in the signature
certificate. An Official Signature serves to facilitate recognition of the fact that a document originates
from a controller in the public sector. It may therefore only be used by this controller in accordance
with the detailed conditions laid down in the following, when signing electronically or drawing up the
documents issued by them: The Official Signature in views of electronic documents shall be displayed
by means of an image which the public sector controller has published on the Internet in secure form
as its own and a reference within the document confirming that it has been officially signed. The
information needed for the validation of the electronic signature has to be provided by the controller of
the public sector.

An electronic document of an authority printed out on to paper is assumed to be authentic in terms of
the laws\[48\] if signed with an Official Signature. The Official Signature has to allow verification by
reconverting the printout of the document into its electronic form or the document must be verifiable by
other means provided by the authority. The Austrian scheme of the verification by reconverting the
printout seems to be rather unique: To avoid any losses/misuse caused by media breaks when
printing out Electronic Documents the scheme allows to verify the authenticity of a printout regarding
all elements of the text by input of the variable portion of the text plus the basic data of the Official
Signature. The printed document includes a reference to the source on the Internet,\[49\] containing the
procedure for reconverting the printout into the electronic form and the applicable verification
mechanisms, or a reference to another verification process:

\[45\] http://elak-ext.a-sit.at.

\[46\] Sec 19 to 21 Austrian E-Government Act.

\[47\] Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG) - Federal Electronic Signature
http://www.ris2.bka.gv.at/Dokumente/ErV/ERV_1999_1_190/ERV_1999_1_190.html.

\[48\] Sec 292 of the Austrian Civil Procedural Act – Zivilprozessordnung, Law Gazette 1895/113,

\[49\] Eg https://www.wien.gv.at/sigpruef/f_pruefer/advcgi/sigpruef/pruefer_start.
Pursuant to Sec 18 of the Austrian General Administrative Procedure Act 1991 (Allgemeines Verwaltungsverfahrensgesetz – AVG)\(^{50}\) Processing Submissions (Erledigungen) in writing have to include a signature by the authority. Is the Processing Submission prepared (!) electronically – even if then issued on paper – the written signature shall be substituted by the Official Signature in terms of the E-Government Act. However, this will be obligatory after December 31, 2010. Nevertheless, this leads / will lead to a very intense use of the Official Signature in the workaday life of the Austrian administrative authorities.

The Austrian E-Government Act stipulates that where an authority is required to submit records to another authority and those records were generated and approved electronically, the duty to submit relates to the electronic original (Electronic Documents). This applies, in particular, to records which are kept in an entirely electronically operated file processing and management system. The Electronic Documents must be submitted in a Standard Format. Standard Formats are such electronic formats which, using the latest available technology, guarantee the best legibility of a document possible, from the point of view of third parties also, during the period for which it is envisaged that the document is to be kept. Where the authority to which the electronic record is to be submitted has authorised an Electronic Delivery Service to receive correspondence addressed to it, the record may also be submitted to that agent, in particular, where proof of submission is required.

Consequently, Austrian eGovernment Applications do not solely rely on Electronic Documents as such, either in the form of files that need to be presented by the Data Subject / user to the application; or in the form of files that are issued to the end user after the conclusion of a transaction, but there exists the freedom of the Data Subject to choose between different means of communication when making submissions to such bodies – however the Austrian E-Government Act stipulates a framework for the electronic communication, that is already in use in numeros applications.

Use of the Citizen Card functions in the private sector

Subject to the Austrian E-Government Act is also the use of the Citizen Card functions in the private sector (Verwendung der Bürgerkartenfunktion im privaten Bereich).\(^{51}\) The generation of an ssPIN for

---


\(^{51}\) For the identification of natural persons in electronic communications with a controller within the private sector, an ssPIN may be derived using the Citizen Card, wherein the sourcePIN of the controller replaces the sector code. This shall be subject to the condition that the controller in the private sector has set up a technical environment in which the Citizen Card can be used and in which
use in the private sector requires the cooperation of the Data Subject with the aid of the Citizen Card wherein the Data Subject must be instructed about the initiation of this function. It is permissible without collaboration of the Data Subject and without using the Citizen Card if an unique identification by means of ssPIN in applications of controllers of the private sector is necessary because (i) the controller has to establish the unique identity of his customers because of statutory provisions and (ii) personal data will be processed and transmitted in ways relevant to the Austrian Data Protection Act 2000 (DSG 2000). However, in such a case the generation of ssPINs may only be carried out by the ssPIN Register Authority.52

The sourcePIN of the Data Subject may not be made available to a controller in the private sector by way of the Citizen Card functions at any time during the generation of the ssPIN.53

The Citizen Card scheme can therefore be used especially in the fields of eBanking, eCommerce and eInvoicing:54 An important feature of the Citizen Card is the electronic identification functionality; it is already used by businesses that offer Internet services when they need to know exactly who the customer is. On web sites that already support the Citizen Card, no PINs etc are needed, the user can simply use his/her Citizen Card to identify himself/herself, which saves the user from having to remember a bunch of username/password combinations. For sensitive transactions, the Citizen Card scheme also provides support for signing content, such as on orders or money transfers, which are then verified on the application server. This ensures that any changes that have been made to the document are detected immediately.

Another field for the use of the Citizen Card scheme are Electronic Invoices (eInvoices – elektronische Rechnungen - eRechnungen): eInvoicing with Electronic Signatures offer security for both the sender and the recipient, because it ensures that the data was not tampered with after being transmitted, and on the other hand such eInvoices are valid in terms of Austrian Tax Laws.55

Furthermore, the Citizen Card can be used “at home”56 for data encryption: The Citizen Card is a tool that enables to encrypt data that shall be send confidentially, and decrypt data that has been sent; A-SIT57 has developed a free tool, “Datasafe Citizen Card – Citizen Card Encrypted (CCE)” (Datensafe Bürgerkarte – Citizen Card Encrypted (CCE)),58 which allows to send and to save confidential documents.

the controller’s sourcePIN is made available as the sector code for generation of the ssPIN; controllers in the private sector may store and use only such ssPINs that have been generated using their own source identification number as sector code (Sec 14 Austrian E-Government Act).

52 Sec 15 para 1 Austrian E-Government Act.
53 Sec 15 para 2 Austrian E-Government Act.
55 http://www.e-rechnungen.at/.
57 http://demo.a-sit.at/.
A Citizen Card with a Qualified Electronic Signature can also be used for electronically signing legally binding contracts - fulfilling the legal requirements for hand-written signatures. The E-Government Innovation Centre (E-Government Innovationszentrum – EGIZ)\textsuperscript{59} makes offline\textsuperscript{60} and online\textsuperscript{61} tools available that makes it possible to sign PDF-documents using the Citizen Card. The tool is offered free-of-charge by EGIZ for installation on a local PC. You can also try it out using their online Web tool.

*Technical background of eGovernment Applications – Portal Group and EDIAKT*

The Austrian approach is that eGovernment can only function efficiently when public authorities work closely together and cooperate on an administration-wide scale. The advantage of the Austrian Portal Group Concept is that many applications are available from a single entry point ("single sign on"). Participation in the portal group is governed by the Portal Group Agreement (PVV)\textsuperscript{62}. This agreement sets out the rights and duties with which the joining partners must comply. This agreement creates an environment of trust between the application providers and the base portal providers, who take care of user management.

Communication within the portal group is managed, both technically and organisationally, by the portal group protocol (PVP) and the use of security classes. Application providers determine which of their applications will be available over which portals. In accordance with all data protection regulations, they specify which administration units and employees are authorised to access which applications and define user roles with according access.

The “big picture” of the Austrian eGovernment communication architecture can be illustrated as follows:

\textsuperscript{59}http://www.egiz.gv.at/
\textsuperscript{60}https://demo.egiz.gv.at/plain/projekte/signatur_im_e_government/pdf_signatur
\textsuperscript{61}http://www.buergerkarte.at/pdf-as/
\textsuperscript{62}The Portal Group Agreement and the application form for joining can be found on the Portal Group page at http://reference.E-Government.gv.at.
The Electronic Data Interchange Format (EDIAKT) was developed as a format for standardising communication between different public institutions (authorities, courts of law, businesses). Although all had record management systems that work with electronic records, business cases, and sub-cases including documents, the objects were specific to the manufacturer of the software and not built according to a uniform standard. In the course of further development of the EDIAKT system and due to increased distribution of the ELAK system, the standard was updated to its current format, EDIAKT II. Data is packaged as EDIAKT objects which are comprised of: (i) meta-data that describes a record, business (sub-)case, or document; (ii) process data for process instances and activities in accordance with the XPDL standard of the Workflow Management Coalition,\(^\text{63}\) (iii) content of the record, business (sub-)case, or document; (iv) procedure-specific data that may be attached to an object.

To satisfy the different requirements of institutions using ELAK, EDIAKT implemented a hierarchical structure with four layers. At the bottom is the document, which contains the file in its original format. If the file is not saved in a standard format, a document with a standard format must be attached. One or more documents are wrapped in a business sub-case. It represents the smallest object in EDIAKT II. This business sub-case may further be wrapped along with other sub-cases in a higher level business case.

Authorities that do not have their own ELAK system can still read EDIAKT packages using the free EDIAKT Viewer. The current version can be used to (i) display all meta-data including process data, (ii) show embedded documents and (iii) verify digital signatures.

EDIAKT is used more than just as an interface between different electronic record systems. It can also be used for internal data exchange between special applications and archive systems. EDIAKT II, together with the EDIAKT Viewer and EDIAKT Creator, and supplemented by the standard document format PDF/A, establishes the basis for the long-term archiving of records.

EDIAKT created a uniform standard for the transmission of record information. The ELAK transaction convention takes it a step further and defines special information and electronic record management

system functions and interfaces for the automated exchange of EDIAKT packages over Web services. This eliminates the need to export EDIAKT packages, save them temporarily and re-import them after they have been successfully transmitted.

Many administrations today are already working with electronic record management systems. Information systems that span all levels of administration, such as central registers, are gaining in popularity. The convention implements a standard that makes it easier to couple diverse information systems together over a product-independent interface and to increase interoperability and integration of management systems. Data that may be used and is needed in administrative procedures can be integrated more efficiently into workflow processes.

For further (technical) details see http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19394.

4.1.2 Electronic documents for the purposes of the implementation of the Services Directive

As shown above, the Austrian E-Government Act stipulates a framework for the use of Electronic Documents (also) for the purpose of the implementation of the Service Directive. Therefore, many components required by the Services Directive already exist, although their actual usage by competent authorities has to be intensified.

Implementation of the Service Directive and Electronic Documents

Currently the legal question of which national procedures fall under the Services Directive is under scrutiny and the screening process is not yet finished.

The procedure by electronic means in terms of Art 8 of the Service Directive will be made available through 9 Points of Single Contact, one for each federal country of Austria (Bundesland).

Whether the applicant has to hand over original documents, certified copies or just simple copies of original copies is also under scrutiny and will to a certain extent depend also on the competent authority involved. At the same time, it is clear that simplification of procedures is the first step for an Electronic Procedure in terms of the Service Directive.

Information by electronic means

Overarching the different levels of the administration the national portal HELP.gv.at currently is the main one-stop-shop for eGovernment information, communication and transaction. As a virtual guide to the Austrian administration it offers information for obligatory target groups like citizens and businesses but also for people with special needs, barrier free (WAI-AAA) and in two languages. The information is clustered in almost 200 life situations allowing for user-centric navigation. HELP.gv.at provides a separate section of specific life events for entrepreneurs and information relevant to
Ebusinesses that want to interact with public authorities in Austria. The Austrian Chamber of Commerce (Wirtschaftskammer Österreich) acts as highly competent content partner for such business related information.

HELP.gv.at also uses advanced ways of content syndication to provide partner authorities with up-to-date, maintenance-free content. All partner websites can include and re-use content of HELP.gv.at at their local sites without having to copy and paste information. Because of the use of standard web technologies this mechanism can also be extended to administrations of other Member States who want to provide up-to-date information about Austrian eGovernment services to their service providers (eg. Art. 21 of the Services Directive) and the EC (eg YourEurope Portal).

A searchable directory service of competent authorities is also part of HELP.gv.at. It contains descriptions of responsibilities and tasks of organisational units as well as contact details, which in some cases are also available for individual staff member.

As a next step the personalisation of content of HELP.gv.at, which includes information as well as official proceedings, will become possible. This will allow offering information specifically tailored to the needs of the users.

Currently not all local authorities in Austria are partners of HELP.gv.at. Especially among small municipalities participation needs to become more widespread.

Nonetheless, HELP.gv.at will not form a PSC in Austria. Therefore, the information provided via HELP will not be the “authentic” information in terms of Art. 7 of the Service Directive but rather complement the information given by the 9 PSCs and add additional comfort. HELP will support in navigating to and finding the correct PSC and – if the user wishes so – directly the competent authority.

Electronic procedures

HELP.gv.at already provides all the services necessary for submitting official applications online. It offers various online forms, electronic identity management using the Citizen Card, e-payment and automatically routes applications to workflow systems or mail boxes for manual processing. Authorities implementing online processes can make use of these functionalities according to their organisational and legal requirements. They can of course also use their own systems; HELP-services thus are an offer for authorities, not an obligation.

4.2 Specific document types

As an introduction to this chapter it is important to stress that the Austrian E-Government Act handles the issue of the electronic validation of certain data in detail in its Secs 16 to 18. As the regulations do not totally overlap with the documents mentioned in the Questionnaire a short overview is provided:
• **Information on Economic Activity as a Self-Employed Person**\(^{64}\)

Electronic validation of the nature of a self-employed activity and of fulfilment of the professional requirements for pursuit of that activity may be obtained from the Documentation Registry by the Austrian Tax Authorities (Dokumentationsregister).\(^{65}\)

Where validation of the data referred to above is required in procedures involving a controller in the public sector (Auftraggeber des öffentlichen Bereichs), the Data Subject (Betroffener) may himself supply it by submitting a copy signed electronically by the Documentation Registry or, at the request of the Data Subject, the controller may acquire it by way of electronic access to the Documentation Register.

• **Data concerning Personal Status and Nationality**\(^{66}\)

Where the accuracy of the data stored in the Central Register of Residents (Zentrales Melderegister) with regard to personal status and nationality (Personenstands- und Staatsbürgerschaftsdaten) has been verified by the local registration authorities by way of inspection of the appropriate documents (Standard Documents - Standarddokumente), those authorities must inform the Central Residents Registry thereof and the fact that the data has been verified shall be noted in the Central Register of Residents in a suitable, electronically legible form. The Data Subject may request that such information be entered even outside a procedure for registration of residence (Meldevorgang) if he provides the registration authority with proof of the accuracy of the registration data by submitting the appropriate documents; the service is successfully online: [https://meldung.cio.gv.at/egovMB/](https://meldung.cio.gv.at/egovMB/).

Where other authorities must determine, as a preliminary question in a procedure, the accuracy of data relating to personal status or nationality which are also registration data, they may, provided that the person concerned has consented to acquisition of the data or that such acquisition through official channels is authorised by statute (amtswegige Datenermittlung), submit an electronic request to the Central Residents Registry in that regard.

The Data Subject may make use of the electronic availability of verified registration data by: (i) consenting to the acquisition of the data required from the Central Residents Registry in procedures in which it is necessary to submit Standard Documents; or (ii) requesting from the Central Residents Registry a confirmation of registration which has been signed electronically with an Official Signature and which states that the accuracy of the individual registration data has been verified.

• **Other Data**\(^{67}\)

---

\(^{64}\) Sec 16 Austrian E-Government Act.

\(^{65}\) Sec 114 para 2 of the Bundesabgabenordnung (Federal Fiscal Code).

\(^{66}\) Sec 17 Austrian E-Government Act.
Authorities (Behörden) or persons on whom public powers have been conferred (mit öffentlichem Glauben versehene Personen, especially notaries (Notare)) shall make public on the Internet the extent to which they are prepared to issue electronic validation of the data stored by them within their area of competence or operations.

Validation which refers to personal data may be issued only to the person concerned himself, or to third parties with the consent of the Data Subject only, unless acquisition of the data through official channels is authorised by statute (amtswegige Datenermittlung).

### 4.2.1 Extracts from commercial registers

The Austrian Commercial Register (Firmenbuch) is a public register operated as an electronic database by the Commercial Register Courts (Firmenbuchgerichte), ie the Viennese Commercial Court, the Civil Court of First Instance in Graz and the seven remaining Courts of First Instance.

The object of the Austrian Commercial Register (Firmenbuch) is the registration and publication of facts regarding commercial entities: eg the existence and name of commercial entities (see below); the representation of the entities, the registration of submission of accounts.

The Austrian Commercial Register consists of “authentic data” (authentische Daten); the Republic of Austria is liable for the accuracy of the (correctly filed) data. The Register is organised in two parts: the “general ledger” (Hauptbuch) and the “document collection” (Urkundensammlung). The “general ledger” includes the general data of the entity (Firmenbucheintragung), eg Commercial Register Identity Number (Firmenbuchnummer), the trade name (Firma), etc. The document collection includes all documents on which the general data of the entity is based, eg articles of association etc. Since the year 2005 all Commercial Register Courts have implemented an electronic document collection.

Inter alia the following entities can respectively – except certain personal undertakings – have to be registered in the Austrian Commercial Register: personal undertakings (Einzelunternehmen); Open Personal Companies (Offene Gesellschaften - OG), Private Limited Partnerships (Kommanditgesellschaften - KG), Limited Liability Companies (Gesellschaften mit beschränkter Haftung - GmbH), Stock Corporations (Aktiengesellschaften – AG), Private Fonds (Privatstiftungen) European Economic Interest Grouping (Europäische wirtschaftliche Interessensvereinigungen – EWIV), Societas Europaea (Europäische Gesellschaften - SE). To every entity a unique Commercial Register Identity Number (Firmenbuchnummer) is allocated that consist of numerics and one letter, eg “FB 123456a”

Everybody has the right to access the Austrian Commercial Register (Firmenbuch) and to request extracts form the register (Firmenbuchabfrage). It is worth mentioning that an electronic excerpt of the
Austrian Commercial Register (Firmenbuch) can be “combined” with an electronic excerpt of the Austrian Central Professional Register (Zentrales Gewerberegister) – see below.

The Austrian Supreme Court ruled that the electronic database of the Austrian Commercial Register (Firmenbuch) is legally protected for the Republic of Austria by the Austrian Copyright Act (Urheberrechtsgesetz).

All key information – also historic data (historische Firmenbuchdaten) – related to the above named entities in Austria is stored in the electronic database of the Austrian Commercial Register (Firmenbuch) and can be accessed for remuneration also via the Internet.\(^\text{68}\) The Austrian Commercial Register (Firmenbuch) includes \textit{inter alia} the following data:

- unique Commercial Register Identity Number (Firmenbuchnummer) and competent Commercial Register Court (Firmenbuchgericht);
- full name of the entity (Firma);
- legal form of the entity (Rechtsform) and date of establishment;
- seat (Sitz) and business address (Geschäftsanschrift);
- date of articles of association and its changes;
- name and addresses of all involved persons (shareholders, general managers, representation, etc)
- Depending on the entity basic financial information, including capital and date of submission of accounts.

Additionally, it is worth noting that one Austria provider of the Austrian Commercial Register (Firmenbuch) – the Telekom Austria AG – is participating in the European Business Register (EBR)\(^\text{69}\) managed by the “European Economic Interest Group” in Brussels.

As mentioned above, everybody has the right to access the Austrian Commercial Register (Firmenbuch) and to request extracts form the register (Firmenbuchabfrage) – also for remuneration via the Internet.\(^\text{70}\)

However, whenever an “official document” (öffentliche Urkunde) regarding the status of the registration of an entity in the Austrian Commercial Register (Firmenbuch) is needed, eg to file it with authorities, an authenticated excerpt (beglaubigter Firmenbuchauszug) is necessary, which can only be issued by courts or public notaries (Notaren).

In this context it is worth mentioning the Supplementary Register (Ergänzungsregister), https://www.ersb.gv.at, in which Data Subjects who are not entered in the Register of Residents (Melderegister) and need not be entered in the Commercial Register (Firmenbuch) nor in the Register of Associations (Vereinsregister) can be entered. The excerpts issued online and free of charge show an Official Signature.


\(^{69}\) See [http://www.ebr.org](http://www.ebr.org).

4.2.2 Criminal records

The Criminal Record (Strafregister) in Austria is a centralised electronic database, which includes all convictions of Austrian citizens or inhabitants by penal courts (strafgerichtliche Verurteilungen). The Criminal Record is run by the Viennese Federal Police Central Bureau (Bundespolizeidirektion Wien) as the “Office for the Criminal Record” (Strafregisteramt), whereas the Office for the Criminal Record is not competent for the extracts from the Criminal Record (also known as “evidence that there is no entry in the Criminal Record” [Strafregisterbescheinigung]).

The extracts from the Criminal Record show (not obliterated) convictions respectively show that no conviction is registered. The competent authorities for issuing extracts from the Criminal Records are in cities the Federal Police Central Bureaus (Bundespolizeidirektionen), in Vienna the Viennese Federal Police Commissariats (Polizeikommissariate), otherwise the major (Bürgermeister). Outside Austria the Representations of the Republic of Austria (österreichische Vertretungsbehörden)\(^{71}\) can issue an excerpt.

The following documents are needed to apply for an extracts from the Criminal Record: (i) the application form\(^{72}\) official photo identification (amtlicher Lichtbildausweis).\(^{73}\) However, there is the possibility to apply for an extracts from the Criminal Record online\(^{74}\) respectively the application-form can be downloaded.\(^{75}\) For the online-application the Citizen Card (Bürgerkarte) is obligatory.

The extracts from the Criminal Record also shows an Official Signature to allow the verification by reconvert the printout of the document into its electronic form:

\(^{71}\) http://www.bmeia.gv.at/en/foreign-ministry/service/austrian-representations-in-german.html

\(^{72}\) http://www.help.gv.at/linkhelp/besucher/db/formularauswahl.formular?id=600

\(^{73}\) http://www.help.gv.at/Content.Node/150/Seite.1500004.html

\(^{74}\) http://www.help.gv.at/cgi-bin/system.pl?label=AntragAusstellungStrafregisterbescheinigung

4.2.3 Extracts from professional registers

Firstly, the Austrian systems distinguishes between professions subject to the Austrian Trade Act (Gewerbeordnung) and “free professions” (Freie Berufe), which are subject to specific profession acts and are (mostly) organised in own professional chambers. Free professions (Freie Berufe) in Austria are medical doctors, pharmacists, dentists, notaries, patent attorneys, attorneys at law, auditors/tax advisers, veterinarians, architects / civil engineers, artists, musicians, writers, interpreter.

Professions subject to the Austrian Trade Act (Gewerbeordnung) are registered in the Austrian Professional Register (Gewerberegister), whereas the members of the “free professions” (Freie Berufe) are registered with their professional chamber (overview: http://www.freie-berufe.at/mitglieder.htm).

As mentioned above, an electronic excerpt of the Austrian Commercial Register (Firmenbuch) can be “combined” with an electronic excerpt of the Austrian Central Professional Register (Zentrales Gewerberegister).

The Austrian Central Professional Register (Zentrales Gewerberegister) is a public register operated as an electronic database by the Federal Ministry of Economics and Labour of the Republic of Austria (Bundesministerium für Wirtschaft und Arbeit), whereas the in the Central Professional Register the data of the decentralised Professional Registers run by the local Federal Authorities (Bezirksverwaltungsbehörden) are merged.


The Austrian Central Professional Register (Zentrales Gewerberegister) includes inter alia the following data:
- full name respectively trade name (Firma) of the entity;
- legal form of the entity (Rechtsform);
- all business addresses of the entity, including further places of business (Geschäftsanschrift und weitere Betriebsstätten);
- chief executive officer of a branch (gewerberechtlicher Geschäftsführer);

• integrated businesses (integrierte Betriebe);
• wording of the trade license (Wortlaut der Gewerbeberechtigung).

However, whenever an “official document” (öffentliche Urkunde) regarding the status of the registration of an entity in the Austrian Central Professional Register (Zentrales Gewerberegister) is needed, eg to file it with authorities, an authenticated excerpt (beglaubigter Gewerberegisterauszug) is necessary, which can only be issued by courts, trade authorities (Gewerbbehörden) or public notaries (Notaren).

4.2.4 Certificates of insurance

The Austrian Federal Act on Agreements regarding Insurances (Versicherungsvertragsgesetz) stipulates that insurance companies (Versicherer) are obliged to deliver a written document, a policy (Versicherungsschein respectively Polizze), about the insurance agreement to the insured person (Versicherten). The insured person generally needs the Polizze to claim any insurance benefit (Versicherungsleistung) from the insurance company. Furthermore, the insurance companies are obliged to provide the insured person with a duplicate of a lost policy (Ersatzurkunde) and copies of the policy, however, on the accounts of the insured person.

However, the Austrian Federal Act on Agreements regarding Insurances does not address electronic Polizzen (ePolizzen).

As the Polizze has to be a written document the insurance companies are of the opinion that they cannot issue any ePolizzen. Please note that it might be possible for Austrian Citizen to enter the written Polizzen into an electronic archive that guarantees the authenticity of the Polizze (regarding the Austrian eArchives see below) for a proceeding in terms of the Service Directive.

4.2.5 Proofs of qualifications

Except the already described Austrian Central Professional Register (Gewerberegister) and the registers of the “free professions” (Freie Berufe) (see above), there exists no register regarding proofs of qualifications in Austria and therefore no common electronic proof of qualifications can be provided.

However, there are Online-Archives that can provide authentic documents and this might be used for the implementation of the Service Directive:
The electronic communication with authentic Electronic Documents between attorneys-at-law and the courts is handled via the Archivum. It is an online electronic archive.

The attorney-at-law entering documents into the Archivum has to use his/her attorneys-at-law's card (Rechtsanwaltsausweis) containing the card-infrastructure for the Citizen Card scheme and a Qualified Electronic Signature.

The attorney-at-law provides the court with the regarding IDs of the documents and the court can access them, whereas the authenticity is secured by the Archivum.

The attorney-at-law can also authorise third parties to access certain documents; the third party has to use for the access a Qualified Electronic Signature.

 cyberDOC, the electronic archive set up by Austria's civil law notaries, went online in the year 2000. Since then all notary deeds in Austria have been stored in this electronic archive. cyberDOC enables electronic legal, documentary and administrative transactions.

Several cooperations with government ministries such as the Federal Ministry of Finance or the Federal Ministry of Justice have been initiated using the cyberDOC-infrastructure for various tasks.

4.2.6 Statements from the service provider

As shown above, the Austrian E-Government Act addresses both directions of communication between public bodies and Data Subjects respectively Service Provider. However, the Austrian E-Government Act stresses the principle of freedom to choose between different means of communication when making submissions.

However, most Austrian eGovernment applications integrate statements made by the Service Provider himself into the websites of the regarding eGovernment application, whereas in a lot of Austrian eGovernment applications it is not obligatory to use the Citizen Card or an Electronic Signature. However, if statements from the Service Provider have to be authentic and/or the identity of the Service Provider has to be verified, the Citizen Card scheme pursuant to the Austrian E-Government Act is used.

Please note that there are several eGovernment applications not (only) using the Citizen Card scheme but other proceedings to verify the identity, eg PINs and TANs, eg the Online Tax Declaration Services (FinanzOnline) uses parallel to the Citizen Card scheme also a PIN scheme.
4.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

4.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

The Austrian approach towards the implementation of the Service Directive is a simple reference model to (existing) eGovernment Applications: The model foresees a portal of the PSCs as an entry point for the user where official applications can be submitted. The applications are then processed by individual back office processes. Supporting these process steps, software modules and standards have been developed that now need to be implemented by authorities:

For the internal back office processes standards for authentic electronic documents exist. The Electronic Data Interchange Format II (EDI AKT II) may be used for the communication between the different (public) institutions (see details above). Therefore, “private organisations” (chambers etc) involved in the implementation of the Service Directive would have at least the possibility to read all documents with the EDIAKT Viewer. However, no specific exchange format will be prescribed by law.

As mentioned above, software tools for applying Electronic Signatures to documents are available online for free. These tools may also be used for the communication of the private organisations (back) to the PSC.

Registers like the criminal record database today provide electronic documents officially signed with an Official Signature. The Austrian E-Government Act foresees that in the future every document sent out by an authority has to bear an Official Signature, which allows for the validation of a document by the recipient and guarantees legal validity of the document even as paper printout. This features will be used for the back-office-communication.

4.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

As mentioned above, HELP.gv.at will not be the PSC in Austria, but there will be 9 PSCs in each federal country of Austria (Bundesland). Those 9 PSC may make use of the infrastructure / information provided by HELP.gv.at and they may implement the Service Directive with a “simple reference model” to (already existing) eGovernment Applications:

The model foresees a portal of the PSCs as an entry point for the user where official applications can be submitted. The applications are then processed by individual back office processes. Finally the result of a procedure is communicated to the applicant via electronic delivery of an official Electronic Document. Supporting these process steps, software modules and standards have been developed in Austria that now need to be implemented by authorities:
For fulfilling the Services Directive all competent authorities have to be able to deliver their notifications electronically – to national as well as to service providers abroad. When using conventional e-mail the successful delivery of a message is not verifiable. Electronic delivery is a secure and reliable way of electronically transmitting official documents. It requires unique identification of the recipient (by Citizen Card/ other interoperable eID from other Member States) and supports delivery modes with or without proof of delivery and/or reception. Since all participants of the electronic delivery are identified there is no factual possibility to distribute spam.

Although conventional e-mail will be used by competent authorities as well, it seems to be clear that there will be cases in which proof of delivery is crucial (see e.g. the principle of “positive silence” in Art. 13 para 4 of the Directive. In cases, an authorisation cannot be granted, the authority will be well advised to use registered e-delivery in order to be able to prove the delivery).

One delivery service, that from the user perspective works similar to a web mail provider, is already operational in Austria (www.meinbrief.at). Although some amendments are necessary, the legal framework for electronic delivery already allows authorities to deliver documents to foreign recipients using their own interoperable eIDs. For finding a technical solution ensuring interoperability between different national delivery systems in a way that users can use their own domestic delivery services to receive documents from administrations of other member states deserves further consideration with the other Member States.

4.4 Assessment – Plans, progress and proposals for further harmonisation

4.4.1 Current plans and progress in the implementation of the Services Directive

Austria is currently preparing the participation in the CIP ICT PSP Large Scale Pilot “SPOCS” (Simple Procedures Online for Cross Border Services (SPOCS)). There, the AT Consortium Partner TU Graz\(^81\) will have the lead for the work package on eDocuments. The overall objective of this work package is to enable understanding and recognition of Electronic Documents, as well as the authentication and validation of Electronic Documents. This leads to the following specific objectives:

- establish an inventory of Electronic Documents used in the large scale pilot;
- develop interoperability concepts for existing Electronic Documents;
- develop common specifications for standard document formats and content;
- develop document validation criteria and models;
- implement open source Electronic Document processing modules for existing Electronic Documents and common specifications;
- implement open source Electronic Document authentication modules;
- evaluate take-up and usage of Electronic Documents and the common specifications in the pilots.

\(^{81}\) [http://portal.tugraz.at](http://portal.tugraz.at)
Regarding an EU wide interoperable system for recognition of eID and authentication that will inter alia allow the use of the Citizen Card in any Member State, Austria is involved in the STORK-project. Such system for recognition of eIDs seems to be practically important for the implementation of the Service Directive in the context of this survey.

4.4.2 Suggestions for further European support initiatives

Austria firmly believes that the topic of Electronic Documents is crucial for the advancement of eGovernment as a whole. Therefore, any activity and initiative supporting the further development of this issue is welcome. Of course, the various activities should use synergies and should be complementary and not duplicate each other. So, for the basic work as well as for studies (legal study on the issuing of Electronic Documents within the Member States and on their acceptance as well as on the legal/evidentiary value of those documents if they are printed out etc.) and piloting, for instance IDABC, could be a good support.

82 http://www.iaik.tugraz.at/content/research/e_government/STORK/.
5 Belgium

5.1 General framework for electronic documents in eGovernment applications

5.1.1 Electronic documents in eGovernment applications

At the federal level, Belgium does not have a generic framework related to electronic documents in eGovernment applications in general. While a relatively large number of eGovernment applications are available to the public, they are regulated and implemented on an ad hoc basis.

Generally, Belgian applications do not rely on electronic documents as such, either in the form of files that need to be presented by the end user to the application; or in the form of files that are issued to the end user after the conclusion of a transaction. Rather, the Belgian approach to eGovernment revolves largely around web services and around establishing trusted relationships between public administrations and selected private sector organisations for the direct exchange of authentic information. Thus, when information needs to be exchanged, typically this will be done through these trusted networks rather than by requiring the creation of a specific electronic document.

Thus, as regards electronic documents, no generic legal framework or technical requirements exist, as electronic documents are not currently in common use in public administrations. Instead, the Belgian eGovernment approach relies very strongly on a limited number of electronic authentic sources, such as the so-called “Crossroads Bank for Enterprises” (Banque-Carrefour des Entreprises / Kruispuntbank van de Ondernemingen)\(^83\). This database contains authentic administrative data of every economically active entity (natural or legal person or other entity) established in Belgium. As the examples further below will show, the Belgian eGovernment strategy revolves around ensuring that these authentic databases contain all required information, and in making these resources accessible to a limited number of trusted parties which have a need to access and use the information.

From a technical perspective, governmental services largely exchange data through a high speed closed network called FedMAN (Federal Metropolitan Area Network)\(^84\). A number of services have been implemented to run on FedMAN, including the so-called Federal Service Bus (FSB),\(^85\) which can be considered a generic electronic portal that is used to access certain web services offered at the federal level. These web services allow duly authorised\(^86\) partners (both in the public and private

---


\(^85\) See [http://www.fedict.belgium.be/nl/informatiseren_staat/de_basis/Federal_Service_Bus_FSB_/index.jsp](http://www.fedict.belgium.be/nl/informatiseren_staat/de_basis/Federal_Service_Bus_FSB_/index.jsp)

\(^86\) Subject to the conclusion of specific service level agreements with each partner, which determine the degree of access to the web services, along with the responsibilities of the partner.
sector) to use certain authentic resources, including e.g. the Crossroads Bank\textsuperscript{87}. This approach to
data re-use will also be used in implementing the Services Directive, as will be discussed further below.

Thus, electronic documents are not generally issued to end users or requested from them in the
context of eGovernment applications, and this is unlikely to change in the near future. From a Belgian
perspective, documents as a whole often constitute an unnecessary intermediate step that can be
eliminated from public processes by correctly leveraging electronic resources. The introduction of
electronic documents to replace paper ones would then not be an optimal step forward in facilitating
the life of end users or in improving administrative efficiency.

5.1.2 Electronic documents for the purposes of the implementation of the Services
Directive

Within the context of the Services Directive, the same approach to documents as outlined above will
be followed: internally, electronic documents will generally not be used. However, it is of course
possible that in some circumstances service providers will need to provide electronic documentation,
and in some cases this documentation will need to be signed. In order to understand the Belgian
strategy, it is necessary to first examine how service providers are currently registered in the relevant
databases.

As noted above, any economically active entity in Belgium must be registered in the Crossroads Bank,
in addition to meeting a number of other formalities (e.g. VAT registration, social security obligations,
showing technical capability through diplomas, obtaining licenses and permits, registering with
professional bodies, etc). In order to assist entrepreneurs in meeting all formalities, a network of so-
called “enterprise kiosks” (guichets d’entreprise / ondernemingsloketten) has been created. Enterprise
kiosks are physical offices which typically also have an on-line presence in the form of a website, in
which specialised staff are available to assist service providers in identifying and meeting their
obligations. They have been authorised to maintain certain information in the Crossroads Bank and
other authentic sources, so that they play a crucial role in registering economically active entities in
Belgium.

Currently there are 9 recognised enterprise kiosks\textsuperscript{88}, all of which have multiple offices across Belgium,
for a total of over 200 physical offices. At this time, the electronic services offered through these
kiosks are limited: while their websites often provide electronic model documents, signed original
forms still have to be presented by the service provider in person to one of the kiosks in Belgium or
sent via traditional mail; thus, fully electronic services are currently only rarely available to the service
providers. The kiosks themselves however can use a certain number of web services offered at the
Belgian federal level to communicate with the competent administrations, e.g. to register companies in
the Crossroads Bank.

\textsuperscript{87} The FSB is the successor of the earlier Universal Messaging Engine (UME), which offered less
inherent support for web services.

\textsuperscript{88} See also http://mineco.fgov.be/enterprises/crossroads_bank/bce_kbo_nl_006.htm
The kiosks assist service providers in identifying the competent professional organisations, and inform the service providers of any requirements for establishment or for providing services. In that sense, the enterprise kiosks can function as a gateway between service providers and any professional organisations that they may need to communicate with. It is clear that their traditional role of assisting service providers corresponds closely to the tasks that the Services Directive foresees for the Points of Single Contact, although obviously the Points of Single Contact must be able to offer their services entirely electronically, which is not currently the case for the enterprise kiosks.

Thus, it is not surprising that the enterprise kiosks are currently planned to take a central role in implementing the Services Directive. As it has already been made clear that the Directive allows multiple Points of Single Contact to be established, it is envisaged that each of the enterprise kiosks would offer the functions required of a Point of Single Contact. While the enterprise kiosks are not public administrations, this shift in their responsibilities would be possible due to the fact that the kiosks have specific contracts with the federal government (specifically with the Ministry of the Economy) detailing their tasks, which are due to be renegotiated next year.

The implementation of the Services Directive is expected to be done in phases in Belgium. So far, the Belgian efforts have mostly focused on finalising the required screening exercises, in which a very strong emphasis has been placed on following the Directive’s requirements for administrative simplification in a strict manner, thus avoiding the need for original documents whenever possible, to minimise problems related to this issue. As was to be expected, the screening exercise thus far has shown that electronic documents are only very rarely used in practice, both by public administrations and by private organisations.

By the end of 2009, the first phase of the implementation is expected to be completed. This will entail a two-fold change, in relation to the tasks of the enterprise kiosks and in the operation and functions of the Crossroads Bank.

The Crossroads bank will be extended to include more information in relation to economically active entities, specifically by increasing the number of authorisations that can be registered. Thus, an entry for a specific service provider would also indicate the specific services that it is authorised to provide, based on the evidence it has presented to the enterprise kiosks.

---

89 See p.19 of the Handbook for the implementation of the Services Directive offered by DG Markt:
“The concept of "points of single contact" does not mean that Member States have to set up one single centralised body in their territory. Member States may decide to have several "points of single contact" within their territory.

The “point of single contact” must however be “single” from the individual provider's perspective (i.e. the service provider should be able to complete all procedures by using only one such point of contact).”
http://ec.europa.eu/internal_market/services/docs/services-dir/guides/handbook_en.pdf

90 From a legal perspective, this issue was already partially addressed through the Programme Law of 22 December 2003, in which article 508 already prohibited federal administrations to request certified copies (but not original documents). This prohibition was also copied at the regional level by the Flemish Region, the Brussels Capital Region and the Walloon Region.
The kiosks on the other hand will be mandated to add or update this information in the Crossroads Bank through a series of web services. As it would not be realistically feasible for each office of the kiosks (which number in the hundreds as mentioned above) to undertake the required implementation efforts, the functionality will be designed and implemented at the federal level by FEDICT\[91\], the Belgian federal Ministry of ICT, through the aforementioned Federal Service Bus. FEDICT will offer a number of web services which the enterprise kiosks will be authorised to use in order to ensure that they can interact with official registers and add or edit the necessary information.

In a second phase, this mechanism will be further refined, including by examining how the enterprise kiosks can more easily communicate with non-governmental organisations such as professional bodies or orders. However, initially the service providers (whether foreign or national) will communicate with the enterprise kiosks via their preferred channel (i.e. via websites, e-mail, telephone, fax, or personal contacts), and the enterprise kiosks will be responsible for ensuring the follow-up with the competent administrations and organisations, and for communicating the outcome to the service provider, as required by the Directive.

In relation to specific electronic documents to be provided by service providers (i.e. in cases where administrative simplification has not resulted in the elimination of the need for original documentation), it is not yet certain what approach will be followed, either with regard to signatures or with regard to documents. For Belgian service providers, the approach is likely to focus on using the signature capabilities of the Belgian eID card, as the rollout is expected to be completed by 2009. For service providers of other Member States, Belgian administrations are currently examining how they can incorporate trusted lists of CSPs into their solutions. However, in order to keep the system manageable, the number of CSPs included in such a trusted list is envisaged to be quite limited (around 15-20 CSPs), as the administration wants to keep the technical efforts required to be able to support these CSPs to a reasonable limit\[92\]. From that perspective, the use of national signature validation platforms (such as the Spanish @firma) is seen as a positive step, as it would increase the number of supported CSPs without increasing the complexity at the national level. With regard to signature level requirements, while the Belgian signature is considered to be a qualified signature, it has not yet been decided whether this will also be required of electronic signatures in the cross border context. Before making this decision, Belgian administrations first wish to see the direction in which European initiatives are evolving to determine how they can easily integrate an optimal number of e-signatures from other Member States while ensuring reliable and non repudiable cross border information exchange.

Regarding the document types to be supported, Belgium is similarly awaiting what trends are emerging at the national level in other Member States. Internally, a substantial number of Belgian eGovernment applications (most notably tax related applications) use Adobe LifeCycle products so that this would also be an obvious choice for the implementation of the Services Directive; however, this is not a certainty yet. Generally speaking, as noted above, Belgian administrations do not require the use of electronic documents from the end users, and thus a large margin of flexibility still remains.

---

91 See [www.fedict.be](http://www.fedict.be)

92 Specifically, the Belgian administrations envisage that the validation of electronic signatures will be done through OCSP lookups. Thus, each additional CSP would require the integration of a new OCSP responders. To keep the total number of responders limited, currently it is planned to support only a limited number of CSPs.
in making implementation choices. If interoperability would require the uptake of a specific standard, it would likely be possible to integrate this, provided that the standard is sufficiently supported at the international level.

From a practical perspective, service providers wishing to become economically active in Belgium using electronic means only will need to contact an enterprise kiosk, each of which will function as a Point of Single Contact. Providing the needed information will initially be limited to relatively low-tech and accessible means, such as on-line web forms for data entry and generic e-mail for transmitting specific documents. As mentioned above, it is not yet clear which document types and signature requirements will be imposed; this depends to a large extent on the evolutions at the European level in the next few months. After that, the enterprise kiosks acting as a Point of Single Contact will be responsible for ensuring the proper follow-up, including by interacting with any competent administrations or private organisations. The processes to be followed in order to do so will of course depend on the requirements of the specific service provider. For instance, the creation of enterprises will require a cooperation to be set up with the Royal Federation of the Belgian Public Notaries\(^{93}\). These workflows are currently being mapped.

With regard to the status of these plans, currently the required legislative changes are being examined, most notably to the Crossroads Bank Act and the regulations in relation to the functions of enterprise kiosks\(^{94}\). Other regulatory changes will be easier to implement, since the Programme Act of 24 December 2002 already gave the government a mandate to change laws for the purposes of administrative simplification, and specifically to facilitate the use of electronic means in communication between public administrations and citizens or businesses (Article 409 and following).

From a technical level, the emphasis is on the development of appropriate web services that can be used by the enterprise kiosks/Point of Single Contact to facilitate their operation. This will include e.g. the development of timestamping services for applications which may require this (offered in collaboration with the Royal Federation of the Belgian Public Notaries) and an e-payment module (in collaboration with Ogone).

\(^{93}\) See [http://www.notaris.be](http://www.notaris.be) or [http://www.notaire.be](http://www.notaire.be)

\(^{94}\) Mainly the Crossroads Bank Act, i.e. the Act of 16 January 2003 creating a Crossroads Bank of Enterprises, modernising the trade register, establishing recognised enterprise kiosks and pertaining to other matters, *M.B.* 5 February 2003.
5.2 Specific document types

5.2.1 Extracts from commercial registers

As noted above, electronic documents are not normally used by Belgian administrations, and the re-use of authentic sources is much favoured. The commercial registers are a key example of this.

All key information related to economically active independent entities in Belgium is stored in the Crossroads Bank, as noted above, which thus acts as the main commercial register in Belgium. Basic information about these entities stored in the Crossroads Bank includes:

- Full name and legal form;
- Unique enterprise number;
- Seat of establishment and date of establishment;
- Activities according to VAT, social security and tax status;
- Management details, including general managers and daily management;
- Basic financial information, including capital and date of deposit of balance sheets;
- List of establishments on Belgian soil.

All of this information is publicly accessible and freely searchable online. Thus, there would not appear to be much added value to issuing extracts, since the most up to date is already freely available through a web interface to any interested party. For this reason, no electronic document exists at this time, nor is one foreseen to be created in the future.

Additionally, it is worth noting that Belgium participates in the BRITE Project, which aims at interlinking European business registers, which would eliminate the need for exchanging extracts.

5.2.2 Criminal records

Extracts from the penal register (also known as a ‘proof of sound behaviour and mores’ (bewijs van goed gedrag en zeden / certificat de bonnes conduite, vie et moeurs) exist in Belgium, but only in a paper format. The extract is provided by the local commune of domicile for natural persons, and by the Attorney-General in Brussels for legal persons.

96 Business Register Interoperability Throughout Europe; see http://www.briteproject.net/
In some communes, the possibility exists to request the extract electronically using the Belgian eID card; however, the resulting document is then still typically delivered by traditional mail in a paper format. Pilot projects exist in which the electronic request results in an electronic (and electronically signed) extract. The electronic certificate can be requested through a web portal (see e.g. http://www.stadmechelen.be/eloket/, the portal of the commune of Mechelen) using the eID card. Following a successful request, a signed PDF-file will be made available to the requesting party via the secured portal, from where it can be downloaded and sent to other parties. The application was created as a joint collaboration between the city of Mechelen, the federal government, IT service provider CIPAL and Adobe. The resulting PDF-file is electronically signed by the competent official at the city of Mechelen, using a Globalsign issued X.509 soft signature certificate which indicates the official capacity of the representative, and there seems to be no reason to doubt its legal validity. However, the pilot has thus far not been generally taken up in other communes, and it is not envisaged that the use of electronically signed pdf extracts will become commonplace in the near future.

Additionally, it is worth reiterating the remaining issues: the electronic certificate can only be issued to natural persons (thus excluding legal entities, who would be a key target audience for the purposes of the Services Directive) who hold a valid eID card (excluding service providers who have no permanent residence in Belgium) and who reside in the issuing commune (excluding communes which have not yet established such a service).

5.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations, orders or stakeholder bodies. While it is difficult to obtain a complete overview, it does not appear that the extracts issued by such private organisations are commonly issued in a paper form. The legal possibility to do so exists, due to the implementation of the Signatures Directive, but in practice only paper documents are commonly issued. In instances where electronic documents are made available to the members of a specific profession, this is typically only done in the form of paper copies, notably PDF scans of the original documents.

Currently, no plans exist to make the use of electronic documents mandatory or to encourage them further. For the purposes of Belgian PSCs, this would likely not be particularly productive, as again the information is typically publicly accessible through the Crossroads Bank public search interface. One of the elements indicated through this site is the "professional qualification" of the service provider, attesting to its acceptance to offer the covered services in Belgium. Again, there seems to be little added value in issuing separate documents attesting to this fact.

---


98 For older entities, established before July 2003, this information is frequently unavailable. However, the Federal Service of Administrative Simplification stresses that the mere inclusion as a commercial entity implies that the Belgian regulation regarding its establishment has been fulfilled. See http://www.vereenvoudiging.be/doc/1205752744-3525.pdf, slide 16.
5.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form. While it would be legally possible to do so under the terms of the eSignatures Act\(^99\), in practice there seems to be no demand for electronic certificates, and so far there are no applications or services that require them, either in the public or private sector. Thus, the only electronic certificates of insurance that are encountered in practice are unsigned scanned documents (typically in pdf or tiff formats), which are occasionally used in cases where originals are not required.

Currently, no plans exist to make the use of electronic certificates of insurance mandatory or to encourage them further. For the purposes of Belgian PSCs, the emphasis is mostly on ensuring that original documents are no longer requested unless this is absolutely necessary, in compliance with the administrative simplification obligations of the Directive.

5.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications: generally, these are private sector issued documents for which only paper originals are available. While electronic copies might occasionally be presented in the form of unsigned scans, this is merely a matter of convenience. No specific rules or framework exist for electronic proofs of qualification beyond the general eSignatures Act, and no plans have been proposed to encourage or mandate their uptake.

5.2.6 Statements from the service provider

Statements made by the service provider himself will likely be integrated into the websites of the enterprise kiosks as web forms to be completed and signed. It is not yet clear which requirements will be imposed on such statements, beyond the comments made above: in all likelihood, a limited number of signature solutions will be supported in cases where signatures will be required.

---

5.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

5.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As was noted above in the explanation of the tasks of enterprise kiosks, the identification of the competent public administrations and private organisations and the interaction with them is already a core function of the kiosks. This will thus remain the same after the implementation of the Services Directive: the enterprise kiosks, acting as a PSC, will still be in charge of identifying the appropriate bodies that need to be communicated with on behalf of the service provider. The main change is of course that the kiosks will also become responsible for interacting directly with these bodies.

With regard to the actual communication between the kiosks and these administrations and/or organisations, it is currently being examined how these can be simplified and modernised, to ensure that the service provider will no longer have to correspond with any other entity than the kiosks. Service providers will provide any needed documentation to the enterprise kiosks, who will then process this information in accordance with the procedures that have been defined for each specific service type.

With regard to interactions with public administrations (such as the registration of enterprises in official databases, VAT registration, registration as an employer, etc.), the enterprise kiosks will be able to use web services which are currently being created and expanded at the federal level, as noted above. For communications with private organisations, most interactions will not be automated, and the kiosk staff will instead contact the competent organisations directly via any appropriate means – which may include e-mail, but also more traditional means such as fax, telephone or even traditional mail – to ensure that the information is processed correctly. This is however a new task for enterprise kiosks, whose legal responsibilities thus far have only included interactions with public authorities.

If service providers of other Member States rely on foreign electronic documentation which is difficult or impossible for the kiosks to validate themselves, it is currently foreseen that this information will be validated through the IMI system\(^\text{100}\). Obviously, this is regarded as a fallback solution which will only be used when needed, and not as a standard practice.

As noted above, while the enterprise kiosks have already been in operation for quite some time, they will not provide the services described above until the required legislative changes have been made, including through an update of the Crossroads Bank Act and through the renegotiation of the contract between the federal government and the kiosks defining their responsibilities.

5.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Currently, the enterprise kiosks all have multiple physical establishments across the Belgian territory, in addition to a single website per kiosk (but not per establishment). As noted above, the websites currently are mostly informative and offered limited possibilities for direct interaction with the kiosks; as such, they cannot currently be considered to be PSCs.

The physical establishments of the kiosks will remain in the future, to ensure that service providers can use the channel of communication which they prefer. However, the web presence of the kiosks will be expanded to ensure that they can be used by the service providers to communicate directly with the PSCs. As noted above, this will require changes both at the legal front (including an update of the Crossroads Bank Act) and at the technical front (by making web services available at the federal level which the enterprise kiosks can use). Elements such as response time requirements, use of specific languages, and liability have not yet been reviewed, although it should be noted that the Crossroads Bank Act already contains certain provisions to this effect (e.g. a rule declaring that all required authorisations from the federal government are deemed granted if no reply is sent by the competent administration within 15 days of the submission of a complete file by the enterprise kiosks (Article 44 of the Crossroads Bank Act), and a requirement for the kiosks to obtain adequate professional liability insurance (Article 45).

With regard to communication with the service provider, no specific decisions have been made at this point yet. However, it seems likely that at an initial stage simple e-mail communication or a similarly accessible technology will be chosen. More complicated and/or highly secured solutions can be considered in the longer term.

When specific electronic documents (such as authorisations or licenses) must be delivered to the service provider, a number of possible solutions are still being considered, and it is not yet clear how this situation would be handled.

5.3.3 The front-office – communication between the Government and the service provider

Like other economically active independent entities in Belgium, the registered service provider will be granted access to its own data in the Crossroads Bank via a web application.
5.4 Assessment – Plans, progress and proposals for further harmonisation

5.4.1 Current plans and progress in the implementation of the Services Directive

As shown in the overview above, Belgium already has an advanced infrastructure in place that can be leveraged for the implementation of the Services Directive, in the form of the enterprise kiosks that already support part of the functions expected of the PSC; and in the form of the Crossroads Bank for Enterprises which acts as an official register of essential information related to service providers, including specific authorisations and fields of economic activity. It is thus not surprising that it is planned to leverage this infrastructure to a significant degree in implementing the Directive.

Specifically with regard to electronic documents, Belgian experience has been limited. This is to a large extent due to the role and use of authentic sources of information as a replacement of paper documents. As noted above, a fundamental principle behind Belgian eGovernment initiatives is that progress can best be made by making a limited number of authoritative electronic resources accessible to specific trusted and mandated organisations. From that perspective, the introduction of electronic documents might be considered a step backwards, as it would constitute a re-shaping of earlier formalities (i.e. turning paper documents into electronic ones), rather than eliminating them.

Thus, while the tasks of the enterprise kiosks and the technical infrastructure made available to them will need to be updated as a part of the implementation of the Services Directive, the uptake of electronic documents is not expected to be a key part of this process. Rather, the existing Crossroads Bank will be extended to include additional information related to the service providers, including the specific authorisations that they have obtained from public or private sector bodies.

This does not necessarily mean that electronic documents would be entirely unused by the Belgian PSCs, but rather that they would not become a key part of the Belgian strategy to implement the Services Directive. If this would turn out to be necessary, it would be feasible to create electronic documents containing the registered information using any number of common standards. However, generally speaking, the Belgian approach much favours the elimination of documents (paper based and electronically) and relying on the creation of trusted networks of authentic information instead, which can be accessed by duly mandated parties through specific web services. As the aforementioned example of BRITE shows, this is a model that could also be applied in a cross border context.
5.4.2 Suggestions for further European support initiatives

Given the Belgian emphasis on authentic sources and web services rather than electronic documents, the creation and expansion of trusted networks to exchange authentic information between mandated parties would seem to be a favoured option. However, as an interim step, Belgium would also welcome further harmonisation of existing electronic documents. From a technical perspective, the Belgian infrastructure would be able to accommodate most widespread standards, so that there is no specific preference in this regard. Similarly, if this would be necessary and beneficial, it would be possible for Belgian administrations to deliver electronic documents as well via web services.

With regard to electronic signatures, it is not yet clear which signature solutions will be supported in cases where signatures will be required. In principle, the Belgian approach is envisaged to support the Belgian eID card and a limited number of certification service providers of other Member States, likely through a trusted list. However, to ensure that implementation efforts are kept manageable, this list should be kept limited in scope (15-20 CSPs are currently envisaged).

It is not yet clear how this approach can be reconciled with the larger number of European CSPs in existence, although possible solutions might include the support of CSPs which are active in a number of countries, or the integration of validation services that would allow a larger number of signatures to be validated. In relation to signatures placed on electronic documents of other Member States, there is an interest in pursuing the option that was tested in Austria\textsuperscript{101}, in which electronically signed documents are also provided with visual information regarding the essential characteristics of the signature and signatory (including specifically his/her legal capacity), along with contact information of the issuing authority. It would appear that this would be a relatively simple step if further harmonisation efforts are undertaken, which would greatly facilitate validation processes.

At any rate, key difficulties in practice include the determination of the reliability and responsibilities of service providers of other Member States, and the ownership of these CSPs, as it may be politically sensitive to support CSPs which are not under public sector supervision. Thus, the issue of electronic signature support is certainly a field where European initiatives could be useful in order to improve trust or facilitate validation of e-signatures.

\textsuperscript{101} See e.g. \url{http://www.a-sit.at/pdfs/20060504%20eID%20Demonstrations.pdf}, slide 11
6 Bulgaria

6.1 General framework for electronic documents in eGovernment applications

6.1.1 Electronic documents in eGovernment applications

The Bulgarian general framework for electronic documents in eGovernment applications consists of two laws – the new Electronic Governance Act (valid as of 13th June 2008) and the Electronic Document and Electronic Signature Act (valid as of 6th October 2001), and several secondary legislative acts related to the implementation of the Electronic Governance Act (EGA).

The Electronic Document and Electronic Signature Act (EDESA) introduces the general rules concerning the use of electronic documents. Furthermore, it generally transposes the provisions of the eSignatures Directive but also lays downs certain specific requirements with regard to the electronic signatures that might be considered as an obstacle for electronic delivery of documents in cross-border situation.

The main differentia specifica of the Bulgarian legislation in comparison to the eSignatures Directive is related to the definitions of different type of electronic signatures. The meaning of electronic signature under EDESA is similar to the meaning of advanced electronic signature under the Directive. Electronic signatures as defined under the Directive will thus not always be considered an e-signature under the Bulgarian law. Electronic signatures under EDESA also comprise the advanced electronic signature and the universal electronic signature, both notions which are given specific definitions under Bulgarian law. The advanced electronic signature under EDESA could be equaled to the “qualified” electronic signature under the meaning of Art. 5, para. 1 of the eSignatures Directive. The universal electronic signature on the other hand is a type of advanced electronic signature which is supported by a qualified certificate issued by a certification-service-provider registered at the Bulgarian Communications Regulation Commission.

According to EDESA, the universal electronic signature is the only type of electronic signature which has the effect of a handwritten signature in respect to everyone, unlike the “basic” and the advanced electronic signature which have such an effect only between private persons. Thus, only the universal electronic signature could be used for eGovernment needs.

Pursuant to Art. 8 of the EGA, the administrative bodies, the persons exercising public functions and the organizations providing public services are obliged to provide all administrative services within their competence in an electronic way, unless the law provides special formal requirements for the performance of certain actions or for the issuance of certain documents. Generally, the new Bulgarian approach to eGovernment is rather oriented to direct exchange of authentic information between the administrative bodies, the persons performing public functions and the organizations providing public services than requiring the creation of a specific electronic document. The E-Governance Act totally
reforms the current administrative practices, particularly regarding the communication by electronic means with the administrative authorities, the persons exercising public functions and the organizations providing public services. Pursuant to the E-Governance Act a significant part of the required documents and data concerning the person applying for an e-government service shall be obtained \textit{ex officio} by the provider of this service directly from the relevant authority which is primary data administrator of the required information.

However, the eGovernance framework, and in particular the Ordinance for the Electronic Administrative Services, determines strict requirements for the formats and the obligatory requisites of the electronic documents. Pursuant to Art. 65 of this Ordinance for the purposes of the electronic administrative services may be accepted the following file formats of electronic documents with non-structured content:

1. file formats with option to include an electronic signature:
   
   a) "pdf" (Adobe Portable Document Format, created by Adobe);
   b) "doc" (Document Format, created by Microsoft);
   c) "xls" (Excel Sheet Format, created by Microsoft);
   d) "eml" (EML Format for electronic mail, created by Microsoft);

2. file formats without option to include an electronic signature:
   
   a) standardised format "p7s" (under PKCS#7 (Public Key Cryptography Standard) of RSA Data Security, adopted with RFC 2315 of IETF (The Internet Engineering Task Force) from March 1998, enclosing in a capsule the electronic documents and the electronic signature ("detached signature");
   b) format "ats", enclosing in a capsule the electronic documents and the electronic signature, as well as other certificates ("time-stamp tokens", "certificate status", etc.);

3. file formats, signed and connected with an electronic signature through "PKCS#7" and "ATS" with included content of the file:
   
   a) "sxw" (created by means of Open Office);
   b) "txt" (text files in ASCII 7-bit format, unicode format, coded in 8-bit UTF-8 or CP1251);
   c) "rtf" (Rich Text Format v1.6, v1.7, v1.8 and the next, text files);
   d) "jpg", "jpeg" (JPEG JFIF v1.02 and the next, raster graphic files);
   e) "j2k", "jp2", "jp2" (JPEG 2000, JP2 or JPX raster graphic files);
   f) "png" (PNG v1.2 and the next, raster graphic files);
   g) "tiff" (TIFF rev. 6.0 and the next, raster graphic files).

The required format for electronic documents with structured content is "xml" format.
Furthermore, the eGovernance framework provides for the establishment of an integral portal for access to the electronic administrative services\(^{102}\) and an integral environment for the exchange of electronic documents between the administrative bodies, the persons exercising public functions and the organizations providing public services (Art. 12 and Art. 41 of EGA).

On the basis of the main official registers in Bulgaria (the Commercial Register, BULSTAT Register and the Unified System for the Registration of the Citizens and the Administrative Services) the EGA determines a unique identification number for each Bulgarian citizen, foreign citizen residing in Bulgaria and each legal entity or other kind of establishment on the territory of the country. Through these unique identification numbers the respective administrative body should be able to request and to obtain the necessary data for the provision of respective administrative service directly, in an electronic way and *ex officio*, from other administrative body/bodies that act as primary administrator(s) of these data.

The plans in respect to eGovernance in Bulgaria elaborate on keeping the official registers and data bases in an electronic form. They are also focused on implementing an electronic flow of most of the documents within the administrations and on switching to full electronic data exchange between the administrations. The new electronic Bulgarian Commercial Register is considered below as an example of this trend.

Thus, the exchange of documents between the citizen/organizations and the administrations will be mostly limited to submission of requests (applications) for administrative services. When given documents should be presented as proofs of evidence, they should be submitted as scanned copies. The final acts of the administration (permits, certificates, etc.) are not likely to be issued in paper or electronic form, since the data resulting from the service would be accessible by all public authorities – the latter will be obliged to request these data by the administrations which create or collect these data first. In this respect the exchange of electronic documents will be more substantial between the very public authorities while requesting data or, respectively, responding to such requests.

### 6.1.2 Electronic documents for the purposes of the implementation of the Services Directive

At this stage, no specific legal requirements regarding the acceptance of electronic documents from service providers are defined, including those from other Member States.

The initial plans point to the eventual use of the integral portal for access to electronic administrative services (eGov Portal) for accessing the Point of Single Contact too. Since most of the competent authorities in the meaning of the Services Directive fall within the scope of EGA provisions it is not surprising that the integral portal for access to the electronic administrative services is currently planned to take a central role in the implementation of Art. 8. Thus, more or less the same principles and concept as for the eGovernance applications could be followed, including in respect to the acceptance of electronic documents from the service providers.

With regard to signature level requirements an amendment to EDESA will be needed in order to ensure at least automatic recognition of the certificates for “qualified” electronic signatures issued by certification-service-providers established in other Member-States.

Regarding the document types to be supported, the requirements applicable for the purposes of the eGovernance applications would be an obvious choice for the implementation of the Services Directive; however, the choice of this approach is not certain so far.

With regard to the status of these plans, the required legislative changes are currently being examined; the drafting and the adoption of a new law is planned for the next year in order to harmonize the current legal framework with the requirements of the Services Directive. The respective proposals for amendment of the legislation will be drafted by the Ministry of Economy and Energy.

However, no concrete steps for the implementation of the Point of Single Contact or for introducing special legal or technical requirements have been undertaken till now.

### 6.2 Specific document types

#### 6.2.1 Extracts from commercial registers

At the present time a radical reform of the Bulgarian commercial register is in process. Since 1\textsuperscript{st} January 2008 the new electronic and centralized Commercial Register is operational and all new entities subject to registration under the Bulgarian Commercial Act, are entered in it. For all legal entities registered at the commercial registers at the district courts before 1\textsuperscript{st} January 2008 a transitional 3-year period for re-registration at the new Commercial Register is established. Thus, at the present moment extracts are issued both from the commercial registers at the district courts and from the new electronic Commercial Register.

The extracts from the commercial registers at the district courts are issued only as paper certificates. On the other hand the extracts from the new Commercial Register are issued both in electronic form and on paper. However, the electronic extracts are not normally used by the Bulgarian administrations yet. Furthermore, the new Commercial Register is publicly available and as far as an entity entered into this register provides its unique identification number, the administrative bodies are obliged to not require any documents or information that is available in the Commercial Register. They have to check and obtain the necessary data directly from the Commercial Register.

At the end of the transitional period for re-registration all key information related to the commercial entities in Bulgaria will be stored in the Commercial Register. Basic information about these entities stored in the Commercial Register includes:
• Full name and legal form;
• Unique identification number;
• Seat of establishment and date of establishment;
• Subject of activity;
• Management details and representatives;
• Capital;
• Other circumstances determined by the law.

The certificates issued from the new Commercial Register are for:

• The current status of the respective entity on the basis of the entered circumstances;
• The entries for certain period of time;
• The announcement for certain period of time;
• Entered circumstance;
• Announcement and/or a copy of an announced act;
• A copy of a document which is a ground for an entry or erasure;
• Lack of an entered circumstance or announced act in the Commercial register.

The electronic certificates issued by the new Commercial Register are signed with a universal electronic signature.

All information entered in the Commercial Register is publicly accessible and freely searchable online\(^\text{103}\). Thus, there would not appear to be much added value to issuing extracts, since the most up to date is already freely available through a web interface to any interested party.

### 6.2.2 Criminal records

Extracts from the criminal records (also known as a ‘certificate showing no previous conviction’ (свидетелство за съдимост) exist in Bulgaria, but only in a paper format. The extract is provided by the regional courts of domicile of the respective natural persons. There are no analogical certificates for the legal entities.

### 6.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations or stakeholder bodies. While it is difficult to obtain a complete overview, it does not appear that the extracts issued by such private organisations are commonly issued in a paper form. The legal possibility to do so exists, due to the implementation of the eSignatures Directive, but in practice only

\(^{103}\) Bulgarian Commercial Register; see [http://www.brra.bg/](http://www.brra.bg/)
paper documents are commonly issued. In instances where electronic documents are made available to the members of a specific profession, this is typically only done in the form of paper copies, notably PDF scans of the original documents.

Currently, no plans exist to make the use of electronic documents mandatory or to encourage them further.

### 6.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form. While it would be legally possible to do so under the terms of EDESA and EGA, in practice it seems to be no demand for electronic certificates, and so far there are no applications that require them, either in the public or private sector.

Currently, no plans exist to make the use of electronic certificates of insurance mandatory or to encourage them further. Furthermore, according to the principles and the provisions of EGA the exchange of authentic data concerning the insurance status between the competent administrations shall be ensured.

### 6.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications. Generally, these are documents for which only paper originals are available. While electronic copies might occasionally be presented in the form of scans, they will be probably signed along with the submitted application, statements and other electronic documents. No specific rules or framework exist for electronic proofs of qualification beyond EDESA and EGA, and no plans have been proposed to encourage or mandate their uptake.

### 6.2.6 Statements from the service provider

Statements of the service provider addressed to the competent authorities will likely be submitted through the integral portal for access to the electronic administrative services – eGov.bg. Web forms will be developed for submission and signing of such statements. It is not yet clear which requirements will be imposed on submitting the statements apart of those, envisaged above. According to the Ordinance for the electronic administrative services, for signing XML based documents for the eGovernment applications, the protocol XAdES (XML Advanced Electronic Signature), formulated in Recommendation TS 101 903 from April 2004 of ETSI (European Telecommunications Standards Institute) and based on Recommendation “XML Signature Syntax and Processing”, adopted by W3C (World Wide Web Consortium) on 12 February 2002, should be used. It is likely that the common requirements applicable to submission of statements under the eGovernance framework, will also apply to statements made by the service providers.
6.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

6.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As mentioned above at this stage no certainty exists on how the Point of Single Contact will be established. The initial plans indicate that the integral portal for access to the electronic administrative services (eGov.bg) is to be used for communication between the service providers and the Point of Single Contact. Since the implementation of EGA is related to the development of an integral environment for the exchange of electronic documents between the administrative bodies, the persons exercising public functions and the organizations providing electronic services, it is likely that this environment will be also used for the purposes of the interaction between the Point of Single Contact and the competent authorities. The integral portal for access to the electronic administrative services is a participant in this environment. Furthermore, this environment is planned to be accessible not only by the public administrations but also by private organizations providing public services, persons exercising public duties and private persons and entities. However, at the present moment the integral environment is in process of development.

The protocol for the exchange of documents through this integral environment will be developed on the base of a specification of the consortium W3C - SOAP (Simple Object Access Protocol) version 1.2 and onwards. The connection between the information systems of the participants in the exchange and the communication server will be performed through a specialized program application for connection (communication client). According to the Ordinance for the Integral Environment for Exchange of Electronic Documents all participants in this integral environment will get access after prior registration. Every participant in the exchange of documents will have a communication client and will sign the messages sent by him with this communication client for the purposes of the communication session. This signature will not have the character of an electronic signature (in the legal sense) and will be used only for ensuring authenticity and integrity of the messages sent for the purposes of the document exchange through the communication client, respectively the communication server. This does not mean that the XML documents (queries) will not be signed by the requesting persons. On the contrary, they should be signed by a universal electronic signature.

However, it is not a certainty yet that the integral environment for exchange of electronic documents will be used for the purposes of communication between the competent authorities and the Point of Single Contact, and much depends on the respective legislative amendments which will be drafted during next year.
6.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

As mentioned above, it is likely the integral portal for access to the electronic administrative services – eGov.bg, to be used for communication channel between the service providers and the Point of Single Contact. Elements such as response time requirements, use of specific languages, and liability have not yet been reviewed. Furthermore, since currently for the access to the electronic administrative services through the portal eGov.bg the use of a universal electronic signature is needed the cross-border communication might be impeded.

With regard to communication with the service provider, no specific decisions have been made at this point yet. However, it seems likely that the general rule for simple e-mail communication as stipulated by EGA will apply.

6.4 Assessment – Plans, progress and proposals for further harmonisation

6.4.1 Current plans and progress in the implementation of the Services Directive

As shown in the overview above, Bulgaria is currently developing its eGovernance framework, and numerous steps have been undertaken in this direction: an adequate legal framework has been recently adopted, an integral portal for access to the electronic administrative services is operational, an integral environment for exchange of electronic documents is in process of development, a new electronic Commercial Register is in place, etc. The development of the Bulgarian eGovernance project is related to the development of an infrastructure that can be leveraged for the implementation of the Services Directive. It is thus likely that the standards and the requirements adopted for the purposes of the eGovernance framework are also to be used for implementing the Directive.

However, as noted above, no certainty exists so far what will be the approach which will be chosen for the implementation of the Services Directive.

Since the competent authorities within the meaning of the Services Directive do not always fall within the scope of EGA, it is unclear whether the concept of EGA and the secondary legislation for its implementation will apply in respect to the communication between the Point of Single Contact, the service providers and the competent authorities.

Enactment of a new law is planned for the implementation of the Services Directive during the next year. Along with the adoption of this new law it is likely that further amendments in the current legislation will be adopted.
Furthermore, the differences between the regime of the electronic signatures under EDESA and the eSignature Directive should be mentioned as an issue which has to be resolved, not only in respect to the implementation of the Services Directive, but also, in general, for overcoming the obstacles to the cross-border electronic communications.

6.4.2 Suggestions for further European support initiatives

With regard to electronic signatures, it is not yet clear which signature solutions will be supported in cases where signatures will be required. As mentioned above, where communication with public authorities requires a signature, currently only the universal electronic signature may be used, i.e. a signature supported by qualified certificates issued by certification-service-providers registered at the Bulgarian Communication Regulation Commission. This approach might be seen as problematic in respect to cross-border communications with service providers from the other Member States. On the other hand, the large number of European CSPs could be also considered as an issue. Possible solutions might include the support of CSPs which are active in a number of countries, or the integration of validation services that would allow a larger number of signatures to be validated. The difficulties in practice include the determination of the reliability and responsibilities of service providers of other Member States, and the ownership of these CSPs, as it may be politically sensitive to support CSPs which are not under public sector supervision. Thus, the issue of electronic signature support is certainly a field where European initiatives could be useful in order to improve trust or facilitate validation of e-signatures.
7 Cyprus

7.1 General framework for electronic documents in eGovernment applications

7.1.1 Electronic documents in eGovernment applications

Cyprus eGovernment applications revolve around eServices and authentic electronic sources. Thus, as regards electronic documents, no generic legal framework or technical requirements exist, as electronic documents are not currently in common use in the public administration.

From an internal public administration perspective, various government departments use an Office Automation System (eOAS) for the electronic management of documents, as well as the automation of the procedures and regulations that rule their creation, archiving, security, distribution and disposal, including their final destruction or long term preservation for future accessibility by the public and researchers.

Features of eOAS include:
- Electronic communication and exchange of electronic documents between the Government Organisations,
- Automatic electronic transfer of important and/or historically valued documents from any Government Organisation to the State Archives
- Accessibility of selected documents to the public.

The above features will be utilised once eOAS is rolled out in all Government Offices and eSignatures are implemented to be used for electronic documents requiring signature. The system is already used in the Ministries of Finance and Foreign Affairs, the House of Representatives, the Central Information Service, the State Archives and a number of other Government Agencies and Departments. It should be noted that Cyprus has transposed the e-signature Directive through the adoption of a framework legislation and is now in the process of developing the required structures and secondary legislation for its effective implementation.

The Cyprus eGovernment strategy revolves around ensuring that Information Systems’ databases contain all required information so as to provide the relevant eServices. It relies heavily on a major key enabler project which is under way, the Government Secure Gateway. The Gateway will provide the core architecture for enabling eGovernment service delivery by providing the tier that enables interoperability, security and authentication, with web-based workflow for interconnection of back-office systems.

Another major project that will be initiated soon is the Creation of a Government Data Warehouse. The objective of the Data Warehouse (central repository of data) is to enable easy access to accurate,
consistent and integrated government data for better and faster decision-making, statistical purposes and for achieving responsiveness to Government obligations.

With projects like the Government Secure Gateway and the Government Data Warehouse, the Cyprus eGovernment Strategy aims to create authentic electronic sources and reuse data where possible, so that the public administration can provide eServices to the public, without asking the citizen to provide information that is already in official registers.

Further to the above, electronic documents are not generally issued to end users or requested from them in the context of eGovernment applications, and this is unlikely to change in the near future.

**7.1.2 Electronic documents for the purposes of the implementation of the Services Directive**

For the purposes of the Point of Single Contact (PSC), the Government of Cyprus has decided to upgrade and expand the existing One-Stop-Shop service which was set up in 2007, under the auspices of the Ministry of Commerce, Industry and Tourism, for local and foreign based companies with the aim of facilitating, accelerating and simplifying the process of setting up a business.

A wide range of services are currently being offered to investors through the One-Stop-Shop which include:
- Provision of information/guidance to potential investors
- Registration of a company
- VAT registration
- Income Tax registration
- Registration with the Social Insurance Fund and Employer’s Registry
- Application for the issue of residence and work permits

Electronic services are not currently available through the One-Stop-Shop.

Through the PSC, Service Providers will be able to complete all necessary procedures and formalities needed with regard to the access to and exercise thereof of a service activity within Cyprus.

The PSC Portal will contain information, online applications, forms/documents to download and related links. Service Providers (whether foreign or national) will communicate with the Cyprus PSC via their preferred channel (i.e. via the Cyprus PSC Portal, e-mail, telephone, fax, or personal contacts), and the PSC will be responsible for ensuring the follow-up with the Competent Authorities, and for communicating the outcome to the Service Provider, as required by the Directive.

The use of electronic documents within the context of the Services Directive will depend on the outcome of the screening of the procedures of the various Competent Authorities.
Currently the screening exercise is in progress. Strong emphasis has been placed on following the Directive’s requirements for administrative simplification, thus avoiding whenever possible the need for original documents, to minimise problems related to this issue.

The screening exercise thus far has shown that electronic documents are only rarely used in practice, both by public and by private organisations.

In relation to specific electronic documents to be provided by Service Providers (i.e. in cases where administrative simplification will not result in the elimination of the need for original documentation), it is not yet certain what approach will be followed, either with regard to signatures or with regard to documents.

For local Service Providers the approach is likely to focus on using the eSignature capabilities of electronic cards once the relevant procedures are in place. For Service Providers of other Member States, it will be examined how trusted lists of CSPs can be incorporated in the solutions to be adopted. The direction, in which European initiatives are evolving, to determine how they can easily integrate an optimal number of e-signatures from other Member States, will definitely affect final implementation in Cyprus.

Regarding the document types to be supported, Cyprus is also awaiting what trends are emerging at the national level in other Member States.

From a practical perspective, Service Providers wishing to become economically active in Cyprus using electronic means only, will need to contact the Cyprus PSC. The means of providing the needed information will initially be limited to relatively low-tech and accessible means, such as on-line web forms for data entry and generic e-mail for transmitting specific documents. As mentioned above, it is not yet clear which document types and signature requirements will be imposed; this depends to a large extent on the evolutions at the European level. After that, the PSC will be responsible for ensuring the proper follow-up, including interaction with Competent Authorities. The processes to be followed in order to do so will of course depend on the requirements of the specific Competent Authority involved.

### 7.2 Specific document types

#### 7.2.1 Extracts from commercial registers

All key information related to economically active independent entities in Cyprus is stored at the Companies Registration System, at the Department of Companies and Official Receiver (D.R.C.O.R) which acts as the main commercial register for Cyprus. The Companies section of the D.R.C.O.R. deals with the registration, follow up, control and striking off of companies, partnerships and business names.
The Companies and Business Enterprises Register contains the following information:

- Full name and legal form
- Unique enterprise number
- Seat of establishment and date of establishment
- Names and addresses of Directors and Secretary
- Basic Financial Information, including capital, date of deposit of balance sheets, Directors Report, Auditors, Report (only for companies)

The registration of European Public Companies (SE) is included in the Register as from July 2007.

Currently, only applications for name approval can be done online. The registration of companies and the filing of company documents will be available online (through the internet) from the Customer’s (or lawyer’s office) as from 2010.

Information in the Registrar’s registry is publicly accessible but it is not searchable online except for the name of the companies. Other information related to commercial registers will be accessible online as of 2010. There will be a fee for every service according to a fee schedule under the relevant Regulation.

Extracts are not currently issued electronically and in view of the plans to have these available through a web interface to any interested party, it is not likely that extracts from commercial registers will be made available in an electronic form.

### 7.2.2 Criminal records

A Certificate of Criminal Record or a Certificate of Clear Criminal Record can be obtained from the Criminal Record Office of the Police Headquarters, following a written or electronic request, made by the person concerned or by his/her authorized representative. The Certificate can be given in person or sent by post in paper format. Electronic certificates are not issued.

### 7.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organizations, orders or stakeholder bodies. While it is difficult to obtain a complete overview, it appears that the extracts issued by such private organizations are commonly issued in a paper form.
7.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form. In practice there seems to be no demand for electronic certificates, and so far there are no applications or services that require them, either in public or private sector. Thus, the only electronic certificates of insurance that are encountered in practice are unsigned scanned documents which are occasionally used in cases where originals are not required.

Currently no plans exist to make use of electronic certificates of insurance mandatory or to encourage them further. For the purposes of Cyprus PSC, the emphasis is mostly on ensuring that original documents are no longer requested unless it is absolutely necessary, in compliance with the administrative simplification obligations of the Directive.

7.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications: generally, these are private sector issued documents for which only paper originals are available. While electronic copies might be occasionally be presented in the form of unsigned scans, this is merely a matter of convenience.

7.2.6 Statements from the Service Provider

Statements made by the Service Provider himself will likely be integrated into the Portal of the Cyprus PSC as web forms to be completed and signed or as attachments. It is not yet clear which requirements will be imposed on such statements. As already stated many issues depend to a great extent on European developments.

7.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

7.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

Most interactions will not be automated in the beginning; the PSC will be in direct contact with competent authorities via various appropriate means – telephone, fax, mail or email with dedicated officers of the competent authorities. Issues relating to the communication between the PSC and the competent authorities are currently being examined and the final structure to be adopted will aim at
ensuring speed and reliability. For some interactions, notably those relating to communication between the PSC and competent authorities belonging to the government sector (such as the registration of enterprises in official databases, VAT registration, registration as an employer, etc.) eServices will be used.

Currently, relevant information regarding the procedures and formalities service providers have to comply with for access and exercise thereof, of all service activities in Cyprus falling within the scope of application of the Directive, whether via establishment or across borders from other member states, are being gathered, along with contact information of dedicated officers for each procedure.

If service providers from other Member States rely on foreign electronic documentation which is difficult for the PSC to validate, it is currently foreseen that this information will be validated through the IMI system or other means.

**7.3.2 The front-office – communication between the Point of Single Contact (PSC) and the Service Provider**

Currently, the One Stop Shop maintains a physical establishment in Nicosia, the capital of Cyprus. The Government of Cyprus intends to maintain a physical establishment for the purposes of the PSC to safeguard that service providers can use the channel of communication which they prefer.

A PSC portal is to be established and designed in such a way as to provide the relevant information on procedures and formalities in a simple, coherent and structured way; i.e. information will be organised by sector of activity. Through the portal, service providers will be able to communicate directly with the PSC. Various solutions are investigated. However, it seems likely that at an initial stage simple e-mail communication or a similarly accessible technology will be chosen. More complicated and/or secured solutions can be considered in the longer term.

It is aimed to include an electronic tracking system, which will be updated by the competent authorities and the PSC, along with the provision of personal space accessible through the PSC portal, whereby service providers will be able to get an overview of their ingoing procedures.

When specific documents (such as authorisations or licenses) must be delivered to the Service Provider, a number of possible solutions are still being considered, and it is not yet clear how this situation would be handled.
7.4 Assessment – Plans, progress and proposals for further harmonisation

7.4.1 Current plans and progress in the implementation of the Services Directive

There is still work to be done for the implementation of the Services Directive. The two basic building blocks relate to the screening exercise and the development of the PSC and electronic procedures both of which are underway. The screening exercise is expected to be completed in April 2009, whilst the necessary legal and administrative changes to be identified by this exercise will follow. With regards to the PSC, the development of the portal is expected to be completed by August 2009. From thereon information will be uploaded so as for the PSC to be operational by December 2009. Beyond these basic steps for compliance with the provisions of the Directive, work is progressing in parallel for a fully fledged longer term solution which includes the implementation of the Government Secure Gateway, the issuance and roll out of the Cyprus eID and the implementation of eSignatures.

Specifically with regard to electronic documents, Cyprus experience is limited. This is to a large extent due to the policy to use authentic electronic sources of information as a replacement of paper documents. As noted above, based on the Cyprus eGovernment Strategy, progress can be made by making a limited number of authentic electronic sources, accessible to specific trusted and mandated organisations.

This does not necessarily mean that electronic documents will not be used by the Cyprus PSC, but rather that they will not become a key part for the implementation of the Services Directive. If this would turn out to be necessary, it would be feasible to create electronic documents containing the registered information using a number of common standards.

7.4.2 Suggestions for further European support initiatives

Cyprus would welcome harmonisation of existing electronic documents.

With regard to electronic signatures, this is certainly a field where European initiatives will be useful in order to improve trust or facilitate validation of e-signatures.
8 Czech Republic

8.1 General framework for electronic documents in eGovernment applications

8.1.1 Electronic documents in eGovernment applications

Presently there is no general framework of legal or technical requirements for electronic documents with the exception of the rules that apply to electronic signatures. Some applications are available as an electronic form, but they are presented on an ad hoc basis by public authorities. In some cases applications can be sent via e-mail as an attachment (e.g. an applications to the Czech Patent and Trademark Office), in other cases it can be submitted via an electronic form available on the authority’s website (e.g. an announcement on personal data processing made to the Czech Office for Personal Data Protection).

The Electronic Signature Act\textsuperscript{104} regulates the legal aspects of electronic signatures. For the purpose of signing electronic documents that are to be submitted in contact with public authorities it is possible to use only advanced electronic signatures based on qualified certificates issued by accredited certification service providers. That applies also to the communication from public authorities to individuals and corporations. So far there are three accredited certification service providers and this number is not likely to change in the near future. The Electronic Signature Act does not stipulate any technical requirements for electronic signatures.

The Czech public authorities are also required to process documents signed with an electronic signature issued abroad. In such a case, the public authority contacts the Ministry of Industry and Trade and the ministry requests the authority of the state involved to verify whether the certificate is valid. Therefore in the context of cross-border communication it is necessary to communicate with the authorities of the states involved. In light of this, the Ministry of Industry and Trade highly recommends creation of a European trusted list of electronic signatures that would not have to be validated.

A draft of a new act is being prepared at the governmental level in connection with the implementation of the Services Directive. This Act on Electronic Operations, Personal Numbers an Authorized Conversion of Documents (the Act on Electronic Operations) will govern the electronic operations of the public authorities involving individuals and corporations and vice versa, and electronic operations among the public authorities. An electronic data box - public mailbox is to be used for this purpose.

The concept of public mailboxes is based on the idea that each public authority and each corporation will be required to have its own public mailbox. Individuals will obtain one at their request only. The mailboxes are to be available free of charge. The communication will then be executed electronically through these public mailboxes. The access to the public mailbox will be restricted to the authorized persons. The electronic public mailboxes are to be established and operated by the Czech Post.

\textsuperscript{104} Act No. 227/2000 Coll. on electronic signature
However, the use of public mailboxes is to be optional, the traditional means of communication (using regular mail, electronic forms or e-mail with an electronic signature) will remain possible.

For electronic communications, electronic documents are to be made available. Thus far only the Register of Trades provides the possibility to obtain an electronically signed extract online. The database of the Commercial Register is also accessible online, however data obtained from the register electronically are not considered original and cannot be used in further communication with public authorities. The new Act on Electronic Operations implements the possibility to convert the original paper documents into an electronic document and vice versa.

As to the technical aspects of electronic documents, there is no general regulation. The public authority that receives the electronic documents can restrict the accepted formats to make sure that it will be able to read the documents using the software and hardware it uses. Each authority is required to publish a list of the accepted formats on its website. The common wide-spread formats (pdf, MS Office document formats and common graphic formats) are usually covered. Some electronic procedures may require completing an online form. Some procedures may require an electronic signature. According to the Czech legislation this means an advanced electronic signature based on a qualified certificate issued by an accredited certification service provider. The qualified certificate has to contain all data necessary to make the person positively identifiable.

To our knowledge there is no soft law (guidelines, recommendations, policies etc.) in the Czech Republic at present.

8.1.2 Electronic documents for the purposes of the implementation of the Services Directive

The concept of public mailboxes is the best possible solution for the implementation of Article 8 of the Service Directive. According to the Ministry of Industry and Trade, a similar concept was introduced in France. However, there is another possibility, namely the creation of a public online portal. This portal will contain all the necessary information and forms needed for the initiation and provision of services. The forms could be completed electronically or a converted document could be attached. Submission would be done with an electronic signature.

The implementation of the Services Directive is expected to be finished by end of year 2009. The Act on Electronic Operations will enter into effect either on July 1, 2009, or on January 1, 2010.

As most of the documents will not be provided in electronic form, the authorized conversion introduced by the Act on Electronic Operations will solve the problem of conversion from paper to electronic documents.
The authorized conversion means:

- the conversion of a paper document into an electronic document, authentication of the content and provision of a verification clause, and

- the conversion of an electronic document into a paper document, authentication of the content and provision of a verification clause.

The authorized conversion will give the converted documents the same legal effects as if they were a verified copy. The electronic documents will be required to be electronically signed and time stamped in order to be converted.

The notaries, regional authorities, registry offices, and some of the municipal offices and representative authorities will provide the process of conversion. The conversion will be provided on request of the applicant for an administrative fee (approximately EUR 4-5 per page).

The technical requirements are not stated yet; the Ministry of Internal Affairs will specify the technical requirements by a public notice.

8.2 Specific document types

8.2.1 Extracts from commercial register and register of trades

The Commercial Register is a public record that contains the data required by law about service providers. The Commercial register is kept by the competent court.

The following service providers are registered: (i) trading companies and societies, (ii) certain foreign entrepreneurs, (iii) individuals who are entrepreneurs and ask for the registration (some registrations are obligatory), and (iv) other entities, if required by special regulation. The subsequent information about the entities is stored in the Commercial Register: (i) firm name and seat / name and place of residence, (ii) the subject of the business, (iii) legal form of the service provider, (iv) registration number / birth identification number, (v) information about the statutory body, (vi) information about the authorized agent, and (vii) other information, if required by special regulation. The Commercial register also contains the Collection of Documents, which contains the key documents relating to the particular entities (e.g. the deed of foundation, the statement of balances, the annual report etc.)

All of this information is publicly accessible online free of charge, however the extracts obtained therefrom are for informational purposes only and can’t be used as original extract obtained from the court – i.e. a valid electronic extract from commercial register is presently not available.
The record proposal can be filed in paper form or through the electronic form available at the register’s website. Electronic signature must be used if the form is submitted electronically.

Once the Act on Electronic Operations is fully operational, authorized conversion of extracts from the Commercial Register will be possible.

According to the information we have received from the Ministry of Internal Affairs, the Czech Republic plans to establish four data registers which will contain the most commonly used data in the public administration. There will be a register of citizens, a register of commercial subjects, a register of properties and the territorial information and a register of rights and duties. The public authorities will use the data from the registers without a need to ask a citizen or a commercial subject to provide this data. Therefore in the future Czech nationals will most likely not be required to submit electronic extracts from commercial register as each authority will have access to all the data which it needs.

Besides the Commercial Register there is also the Register of Trades that keeps record of service providers. The Register of Trades is operated by Trade Licence Offices and is available online. So far the Register of Trades seems to be more advanced in electronic matters than the Commercial Register - from the Register of Trades it is possible to obtain an electronically signed extract. It is also possible to send electronically signed applications to the Trade Licence Office, however, the representatives of the Ministry of Industry and Trade have stated, that this possibility is, as they have learned from their own experience, rather theoretical, as the staff of the Trade Licence Offices is usually not adept in using the technology.

8.2.2 Criminal records

The Criminal Register in the Czech Republic includes only individuals. According to the Czech law, corporations do not have a criminal liability and they are not capable of committing a crime, therefore no corporations are included in the Criminal Register.

An extract can be issued in paper form only. The Criminal Register in Prague and some of the Czech POINTs provide these extracts. The applicants can obtain the extract by visiting appropriate authority personally and filing the application. Czech POINTs issue the extract immediately, while other institutions only send the application to the seat of the Criminal Register and the applicant receives the extract by post.

Filling of an electronic application for the extract from the Criminal Register was not possible until recently. It is possible to require an extract from the Criminal Register by filling in an online form, signing it electronically, and sending it to the Criminal Register.

The draft of the Act on Free Movement of Services enables public authorities to view the criminal record in order to validate the integrity of the service provider. The service providers then do not have to submit their extracts from the criminal register because the public authority can verify the necessary
data online. The Act on Free Movement of Services is expected to become effective before the end of 2009.

As to the technical standards of electronic signatures used by public administration (where it concerns the Commercial Register, Register of Trades and Criminal Register), the approved technical standard is PKCS#7. The validity of electronic signature can be determined by means of the certificate revocation list (CRL). So far no stamping services are required, but once the authorized conversion is introduced by the Act on Electronic Operations, the electronic documents will be required to be electronically signed and time stamped in order to be converted.

8.2.3 Extracts from professional registers

Professional registers are kept by private entities. Most of the professional registers are available online for informational purposes. Extracts from professional registers, however, are usually provided in paper form.

There is currently no incentive to make the use of electronic documents common in this field, particularly because submission of an extract from a professional register is often not an obligatory condition in order to become a service provider.

8.2.4 Certificates of insurance

Certificates of insurance, to our knowledge, are not provided in electronic form. Even though it is legally possible due to the Electronic Signature Act, there is no effort to make the use of electronic documents more common. Particularly, because submission of a certificate of insurance is not a common required condition in order to provide services.

8.2.5 Proofs of qualification

Much as the Extracts from professional registers and Certificates of insurance, proofs of qualification are usually issued in paper form by the relevant institution. To our knowledge, no specific regulation applies to proofs of qualification besides the Electronic Signature Act and there are no further plans for regulation.
8.2.6 Statements from the service provider

Statements from the service provider are usually submitted in paper form. Because of the Electronic Signature Act, it is also possible to submit an electronic statement, however this is not a very common practice.

Public authorities that accept the electronic documents can restrict the accepted formats in order to make sure that they will be able to read it using the software and hardware that they use. Each authority is required to publish a list of the accepted formats on its website. Most common widespread formats will be acceptable.

If public mailboxes are introduced, the service provider will be able to file the statements in electronic form using its public mailbox without the need to sign the statement electronically. As mentioned above, this way will be optional as well as the usual paper-form statement.

8.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

8.3.1 Points of Single Contact

The Services Directive requires member states to establish PSCs. There are already similar points established in the Czech Republic – the Czech POINTs (the Czech Posting Verifying Informing National Terminal, Český podací ověřovací informační národní terminál). It is an assisting point of public administration where it is possible to receive official extracts from the Commercial Register, Professional Register, Criminal Register and Real Estates Register. These extracts were formerly provided by its own authority.

The Czech POINTs are presently situated in more then 2800 municipal and regional authorities (56%), in some branches of the Czech Post (28%), in the offices of the notaries (12%), in the foreign representative bodies and in the offices of the Economic Chamber. Therefore, the Czech POINTs are easily available and highly used by the public. It is expected by the end of 2008, nearly one million extracts will have been issued at Czech POINTs.

The Czech POINT website offers the possibility of electronic application for extracts from the Commercial Register, Register of Trades and Real Estates Register. The extracts are sent back to the applicant by post in paper form.
Surprisingly, the Czech government does not intend to authorize the Czech POINTs to become the PSCs within the meaning of the Services Directive. A new network of PSCs will be established. The PSCs will be physically based by the regional Trade Licensing Offices, i.e. 14 PSCs in the country, and one special superior PSC Office, which will supervise the PSCs and will reside within the Ministry of Industry and Trade.

In addition, one of the PCS will be an electronic application, where the potential service provider will be able to request permits necessary for provision of services. Whether this will be done using public mailboxes or messages signed electronically is still yet to be determined, however the latest draft of the Act on Electronic Operations leans to the use of public mailboxes. This application will be available in multiple languages and will save time and energy for local applicants as well as applicants from abroad.

The online PSC should encourage the use of e-government services and authorized conversion of documents. The online PSC will mediate the delivery of the applications for license to provide services between the applicant and the public authority. Furthermore, it should provide all information listed in Article 7 of the Services Directive.

In order to regulate the delivery mechanisms, it is not necessary to change the current legal framework, as provisions applicable for delivery through electronic mailrooms will apply.

8.3.2 The back-office – communication between the Point of Single Contact and the competent public administrations or private organizations

The idea is that the electronic system of the PSC will resend the application to all institutions involved. This should be processed automatically through public mailboxes.

The PSC will not judge the completeness or accuracy of the application. It will have no competence to issue decisions in the matter. The PSC will be acting only as a dispatch service.

8.3.3 The front-office - communication between the Point of Single Contact and the service provider

The communication from the public authority to the service provider will not go through the PSC. The public authority may choose to use mail, public mailbox, telephone or other appropriate means to answer the submitted application.
8.4 Assessment – Plans, progress and proposals for further harmonization

8.4.1 Current Plans and Progress in the implementation of the Services Directive

There are two acts in the process of adoption: the Act on Free Movement of Services and the Act on Electronic Operations. Both of them are expected to be in effect before the end of the year 2009. As previously mentioned, most likely the system of public mailboxes will be introduced, with the possibility to convert paper documents into electronic documents and vice versa.

The PSC network will have to process hundreds of particular services involving many institutions that must engage into a permitting procedure. A screening of valid legal regulation was carried out recently and all the institutions that will need to be incorporated into the network were identified. What the implementation team seems to struggle the most with is the technical solution of the e-government network. The creation of the electronic PSC network is, especially due to the number of institutions involved and the safety requirements, a considerable challenge.

A minor complication is present due to the fact that two agencies are involved in the implementation of the Section 8 of the Services Directive – the Ministry of Internal Affairs (the technical implementation of Article 8 of the Services Directive, i.e. most likely the matter of public mailboxes) and the Ministry of Industry and Trade (all other issues). The necessity of time for communication between these bodies prolongs the whole implementation process.

In the future the Ministry of Industry and Trade will aspire to integrate more public and private professional authorities into the PSC once it is established.

8.4.2 Suggestions for further European initiatives

Because some the electronic documents will have to be sent cross-border the Ministry of Industry and Trade recommends creation of the technical requirements on the European level. So far the Czech authorities are able to process the most of commonly used formats.

Creation of a European trusted list that would facilitate the verification of electronic signatures from abroad would definitely benefit the system.

Also the representatives of the Czech Ministry of Industry and Trade attended a conference in Baden-Württenberg, where the delegates of present countries and regions shared, among other, their achievements in implementation of Article 8 of the Services Directive. The representatives of the Czech Ministry of Industry and Trade believe that a similar conference organized by the European Commission could be very beneficial for the implementation process in the Czech Republic.
9 Denmark

9.1 General framework for electronic documents in eGovernment applications

9.1.1 Electronic documents in eGovernment applications

Denmark does not have a generic framework related to electronic documents in eGovernment applications in general, i.e. requirements concerning standards, security, and authentication. However, the business portal Virk.dk provides guidelines and a set of best practices towards developing user-friendly forms and applications. Additionally, applications and forms that are to be integrated to Virk.dk will need to incorporate electronic signature by 2009.

Electronic documents already play an important role in eGovernment. They exist alongside traditional paper documents. To a large extent forms etc. are available in editable PDF document that may be printed and sent traditionally or to a large extent submitted electronically by e-mail. A number of applications are based on web services where information is exchanged by input and access to databases. Inputs are usually based on electronic signature (OCES105) and/or PIN codes.

Since January 2008 it has been mandatory for the public administration to use certain open standards. Seven sets of open standards have been adopted. This includes a requirement to receive documents in ODF and OXML. Generally, the public administration also accepts documents in PDF and DOC formats. At this point in time there is no generic legal framework or technical requirements concerning electronic signatures and encryption of authenticated electronic documents sent to the public administration. However, the public administration has since the 1st of February 2005 been obliged to be able to handle OCES electronic signatures. It is, however, only an option for people and businesses.

The business portal (www.virk.dk)

All forms that businesses have to send to the public sector are available electronically on the business portal www.virk.dk. 90 pct. of all the forms sent to the state level of the public sector can be sent fully electronically via the business portal and using single sign-on. The rest can be sent using pdf forms. By the end of 2009 the goal is to reach 100 pct. for forms from both the state and the local government level.

Center for Virk.dk – an office in the Danish Commerce and Companies Agency - manages and controls the business portal and handles communication with the parties interested in the portal such as companies, local and national authorities.

The overall objective of Virk.dk is to relieve Danish companies from administrative burdens and to provide a single entrance to the public sector. This is obtained by making it easier for companies to find business forms and applications to the public sector and information from the public sector.

By servicing 90 pct. fully digital solutions, companies will be relieved from administrative burdens. One can find every business related form from any given authority in Denmark at Virk.dk. By using a digital signature companies can gain direct access to a number of specified services and online

---

105 See below.
administrative systems. Furthermore, Virk.dk provides the search infrastructure across all government web pages to enable users to find all business relevant information at Virk.dk.

The purpose of Virk.dk is to meet the needs of businesses and ease communication with local and national authorities.  

**Electronic Signatures (OCES)**

The Danish Government launched a programme to issue free digital signatures as a means of user authentication for all citizens, with a view to accelerate the take-up of eGovernment services. Generally speaking, Denmark has a very well-functioning digital infrastructure based on digital signature and with numerous available applications.  

The full list of services using the official digital signature (OCES) is published at the website: [www.digitalsignatur.dk](http://www.digitalsignatur.dk).  

The OCES system is tied to the Danish social security number (CPR) and Danish business register (CVR). This is not a problem for foreign citizens establishing themselves in Denmark as they can/must acquire such numbers. The situation is the same for foreign services providers registering with the tax authorities or the Danish Commerce and Companies Agency.

Service providers who are not registered will not have a Danish CVR number, and can thus not benefit from the current infrastructure. A specific task force has been established to address this challenge under the Danish Enterprise and Construction Authority (»Erhvervs og Byggestyrelsen«) and the National IT and Telecom Agency (»IT- og Telestyrelsen«). This work is initiated on the background of Article 8 of the Service Directive.

9.1.2 Electronic documents for the purposes of the implementation of the Services Directive

There is an Internal Market Centre under the Danish Enterprise and Construction Agency. A range of functions related to the Single Market are collected in the Internal Market Centre. First of all, the Internal Market Centre helps citizens and businesses in the Single Market through the European SOLVIT network (free of charge). The Internal Market Centre coordinates the implementation of the Services Directive in Denmark.

A Single Point of Contact (»kvikskrane«) is about to be set up as part of the business portal www.virk.dk. Also, a phone-service with direct access to personal counselling will be established. The service comprises guides and outlines concerning necessary requirements and authorisation schemes. It also includes relevant forms for foreign businesses. This information will be available in...
English. The staff will also pass on applications to relevant authorities in Denmark, and follow-up in order to secure timely answers.

To facilitate the implementation process, the Internal Market Centre has set up a working group with the participation of the ministries affected by the Services Directive. The working group meets on a regular basis to discuss the Directive. The screening of Danish legislation concerning services is also conducted in the working group. Currently the work revolves around the translation of relevant forms and documents, and the establishment of the Single Point of Contact. There are currently no plans to set-up standards for secure (authenticated) documents since non-secured documents are widely accepted in practice.

The Single Point of Contact will be established as part of Virk.dk, and is to be launched no later than 28 December 2009. Translated documents are expected to be uploaded this summer (2009).

The solution for electronic documents in the Single Point of Contact will be based on PDF documents. As mentioned above, the Danish Central Administration already has a tradition for accepting a number of document formats, including PDF-scans. This also relates to documents concerning insurance and certificates. Most offices in the Danish Central Administration are likely to send out scanned certificates by e-mail etc. upon the request of the applicant. This is currently not coordinated. The working group has decided to consider how to deal with authenticated documents sent from Member States where such documents are used. However, no solution is currently found.

Regarding the document types to be supported, Denmark is similarly awaiting what trends are emerging at the national level in other Member States. Danish administrations do not require the use of authenticated electronic documents from the end users, and thus a large margin of flexibility still remains in making implementation choices. If interoperability would require the uptake of a specific standard, it would likely be possible to integrate this, provided that the standard is sufficiently supported at the international level.

9.2 Specific document types

9.2.1 Extracts from commercial registers

The Central Business Register (»CVR« or »det Centrale Virksomheds Register«) is the central register containing primary data on all businesses in Denmark, regardless of economic and organizational structure.

CVR was established on the basis of legislation and The Danish Commerce and Companies Agency is responsible for the daily operation of CVR. It is a general administrative register based mainly on data from the following sources: The Central Customs and Tax Administration, The Danish Commerce and Companies Agency, The National Labour Market Authority, The National Working Environment Authority and Statistics Denmark. The authorities collecting and updating the information are integrated online with the CVR system to ensure that the information is always up-to-date and of high quality. Most data in CVR are publicly accessible.

CVR covers both public and private businesses. In addition, CVR contains detailed information on all private and limited companies and the information is available for purchase and can be downloaded from its website. Non-Danish speaking users are recommended to access the European Business
Registry for an access to information on Danish companies in their native language.¹¹¹ There is provided limited guidance and support via either email or phone for businesses that need to obtain data from the CVR system.¹¹²

The Central Business Register provides among other things the following information:

- CVR number (vat and business registration number)
- Founding date and (if possible) date of termination
- Name and possible subsidiary name
- Primary address and other contact details
- Articles of association
- Branch of trade
- Legal form
- Credit information
- Number of employees
- Opt-out option for promotions and advertising geared towards new businesses
- Possible company information, including financial information

All of this information is publicly accessible and freely searchable online. Thus, there would not appear to be much added value to issuing extracts, since the most up to date information is already freely available through a web interface to any interested party.

The regulation concerning this register is found in the Danish Act on the Central Business Register.¹¹³ It is provided in Section 14 (2) that all public entities except from special situations must use electronic communication when providing and retrieving information from the register. There is no similar requirement for businesses.

¹¹¹ www.ebr.org/.
¹¹² CVR, Erhvervs- og Selskabsstyrelsen, Kampmannsgade 1, 1780 København V, cvrweb@eogs.dk, www.cvr.dk.
¹¹³ Consolidated Act No. 653 (15 June 2006), »lov om Det Centrale Virksomhedsregister«.
9.2.2 Criminal records

The Danish Central Criminal Register (»Kriminalregisteret«) is maintained by the Danish National Police (»Rigspolitiet«). The police may provide three different extracts for private purposes, public purposes, and for use in organisations with kids (»børneattester«). There is no (public) criminal register in Denmark for legal persons.

A private person or a business can request a »private extract« from the local police authority. The »kids extract« can be required by public authorities, private businesses, sports- and other organisations. Criminal records are regulated in the Danish Act on Personal Information in the penal register.

A request for a »private extract« or a »kids extract« can be requested from the local police authority. A consent from the person involved is required. The form for obtaining the consent is available on-line in an editable PDF, which must be printed and submitted physically according to the official information. However, requests per e-mail are also accepted in practice.

Extracts from the penal register exist only in a paper format in Denmark. The extract is provided by the police. The extracts are only sent by traditional mail. I have been informed about a working committee under the Danish National Police (»Rigspolitiet«) which is looking into the possibilities in requiring extracts electronically. However no conclusions or solutions have been formulated yet.

9.2.3 Extracts from professional registers

The Internal Market Centre under the Danish Enterprise and Construction Agency has identified a number of professional registers in Denmark which are covered by the service directive. These registers are primarily maintained by the Danish central administration. It is not possible for the purpose of this report to provide an exhaustive overview of registers and requirements. The registers are maintained by approximately 15-20 authorities, including in particular Danish Commerce and Companies Agency (»Erhvervs- og Selskabsstyrelsen«) and the Danish Safety Technology Authority (»Sikkerhedsstyrelsen«).

---

114 www.politi.dk. See also specifically www.politi.dk/da/borgerservice/straffeattest/straffeattester/ (in Danish).
115 Sexual offences concerning children under 15 years of age.
116 Consolidated Act No. 218 (27 March 2001), »Lov om behandling af personoplysninger i Det Centrale Kriminalregister«.
117 Information has been obtained from: Lise Lotte Christensen, Head of Division, The Danish Central Criminal Register (»Kriminalregistret«), and Mette Tjalve, Chief Assistant Constable (»vicepolitimester«), The Danish National Police.
118 This information has been provided informally as the relevant note has not been completed and is thus not yet ready for release.
119 www.sik.dk.
As mentioned above the solution for electronic documents in the Single Point of Contact will be based on PDF documents, and the Danish Central Administration already has a tradition for accepting a number of document formats, including PDF-scans. This also relates to documents concerning insurance and certificates. Most offices in the Danish Central Administration are likely to send out scanned certificates etc. upon the request of the applicant. This is currently not coordinated. The working group has decided to consider how to deal with secure documents sent from Member States where such documents are used. However, no solution has currently been formulated yet.

Initiatives have been taken to try to lift some of the authorisation schemes in connection to the implementation of the service directive. However, no solution has been settled yet.

The Danish Commerce and Companies Agency regulates the following liberal professions: certified translator and interpreter, accountants, and real estate agents. It also administers a central professional register for people and businesses involved with foodstuff – the so-called »Næringsbasen« (trade register).

Foodstuff

All businesses, who sell foodstuffs for more than DKK 50,000 (EUR 6,667) must as a starting point be registered in »Næringsbasen«. Foodstuff is interpreted to include beer, wine, soda, candy etc. The register includes businesses who provide storage or transportation of foodstuff. The register is maintained by Erhvervs- og Selskabstyrelsen (»Danish Commerce and Companies Agency«). Registering in Næringsbasen may be done on-line using digital signature (OCES) or by submitting a form available in editable PDF. Information may be retrieved electronically (on-line) based on CVR number, business' or owner's name, or address.

Certified translator and interpreter

Certain translators may be appointed as certified translators and interpreters (»translatør«). A certificate is issued by the Danish Commerce and Companies Agency. In order to receive such a certificate, the translator must apply in writing using a form available in editable PDF, which is to be signed and delivered physically together with particular documents. The certificate is only available in paper format.

Auditing and accountants

All businesses who carry out commercial activity as registered public accountant (»registreret revisor«) or state-authorized public accountant (»statsautoriseres revisor«) must be registered in the Danish accountant register (»Revireg«). The register comprises information about the businesses, branches, and where the accountants are employed.

Registration to Revireg must be done electronically at www.virk.dk/revireg using a digital signature (business signature or personal signature if not registered in the Central Business Register [CVR]). Registration in writing (physically) may be sent to the Danish Commerce and Companies Agency if the

120 http://www.eogs.dk/graphics/publikationer/blanketter/startblanket_naeeringsbasen.pdf
121 http://www.eogs.dk/graphics/_ny%20eogs/Love%20og%20Regler/Translat%F8rer%20og%20tolke/ansogn.transl.pdf
business is not registered in Central Business Register (CVR). Information about the registration may be retrieved on-line from Revireg. Revireg is part of Virk.dk.

Property agents

Property agents is a regulated profession in Denmark. The primary regulation is found in the Danish Consolidated Act No. 1073 (2 November 2006) on Real Estate Trade. Only registered property agents may use the official Danish title for property agent (»ejendomsmægler«). For property agents not established in Denmark, but in Switzerland, or an EU or ECC state, and who wish to establish themselves permanently or in order to temporarily provide services as property agents, the registration requirement is found in Section 25 a, and in Executive Order No. 1307 (23 November 2007) concerning registration of Property Agents etc., established in an EU state, in an EEA country or in Switzerland.

The executive order concerns both the permanent establishment and the temporary or occasional exercise of business activities in Denmark as a property agent. Prior application is necessary before carrying out commercial activity as a property agent in Denmark for the first time. A written application must be submitted to the Danish Enterprise and Construction Authority. The application must be accompanied by a number of documents.

There is no system or firm administrative practice for how applications may be submitted electronically. As a starting point, the authority may require the application in print. However, the administration is not refusing the possibility that application may be submitted by e-mail. It should be noted that for the registration concerning a permanent activity, the authorities to a large extent relies on photocopies of official documents rather than originals or certified copies. Thus the use of scanned PDF is not likely to give rise to problems.

9.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued or required in an authenticated electronic form. While it would be legally possible to do so, in practice there seems to be no demand for such electronic certificates. So far there are no applications or services that require them, either in the public or private sector. Currently, there are no plans to make the use of electronic certificates of insurance mandatory or to encourage them further.

Some insurance companies are looking into possible savings in relation to electronic communication with their customers, including the provision of electronic certificates. [At least] one company has

\[\text{Source: } \text{Forsikring & Pension} \]

---

122 Section 3 of order No. 666 (26 June 2008) concerning Revireg.
123 www.revireg.dk.
124 Subsequent amendments to this act include in particular Act No. 123 (13 February 2007) which implements parts of directive 2005/36/EC (7 September 2005) on the recognition of professional qualifications.
125 Erhvervs- og Byggestyrelsen, (Danish Enterprise and Construction Authority), Dahlerups Pakhus, Langelinie Allé 17, 2100 Copenhagen Ø, www.deaca.dk.
126 Information has been received from Gitte Danelund, Danish Insurance Association (»Forsikring & Pension«). She did not have knowledge to initiatives, but no thorough analysis in the business was made.
established a brand which is directed to people who want to communicate electronically.\footnote{Codan Insurance’s brand: Atava, www.atava.dk.} However, the certificates of insurance are delivered in locked, but not signed, PDF documents. The insurance company stores an electronic copy in its own files.\footnote{Information has been received from Paul Færge Winther, Codan Forsikring A/S (insurance company).}

### 9.2.5 Proofs of qualifications

Reference is made to the part concerning »extracts from professional registers«. Proofs of qualifications may be submitted as PDF-scan. Currently such documents are only issued in paper form. Upon request, public authorities may sent the documents as PDF without further security measures. To some extent qualifications are noted in registers with on-line access.

There are no actual plans to develop standards for electronic qualification documents.

### 9.2.6 Statements from the service provider

Statements made by the service provider himself will likely be integrated into the websites of the Single Point of Contact (at the intended counterpart to »Virk.dk«). Information may be typed into web forms, and documents may be attached in various popular formats (ODF, PDF, DOC etc.).

For the report of tax figures, the Danish Tax Authorities\footnote{www.skat.dk.} has its own system which accept both OCES signatures and PIN codes. Based on the experience from Virk.dk, it is likely that the Single Point of Contact will only rely on OCES signatures and not PIN codes. The signature solution is likely to be the official OCES certificate. Such documents may also be attached to e-mails, including forms in editable PDF format (signed or unsigned).

As for foreign businesses without an OCES signature, the situation is not clear. It is, however, likely that documents under these circumstances may be submitted to the Single Point of Contact as attachments to an e-mail. Only businesses who are not registered in the Danish Central Business Register can at the moment not get an OCES signature. At the current stage, this is not likely to change.
9.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

9.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

The Danish »Kvikskranken« will serve as Single Point of Contact. A task-force, under the Danish Enterprise and Construction Authority (»Erhvervs og Byggestyrelsen«) and the National IT and Telecom Agency (»IT- og Telestyrelsen«), has identified the relevant public administrations. The relevant public administrations have access to upload their forms and documents to the website of the Single Point of Contact.

When information, including documents, is submitted to the website of the Single Point of Contact, it will be sent directly to the relevant authority. If the information is sent via e-mail to the Single Point of Contact, it will »manually« (i.e. after processing by a competent official) be transmitted to the relevant authority.

FESD

In early 2004 the Danish authorities appointed vendors to deliver a Government-wide electronic document management system, called Joint Electronic Document Management System (»FESD«).

The objective of the FESD project is to increase gains in quality and productivity by encouraging public bodies to introduce fully digitised procedures. Effective project management and change of work processes are therefore some of the pillars supporting the FESD project. The overall aim of the FESD project is for more public organisations to become digital, and as a result, to profit both in terms of higher efficiency and better quality.

On the one hand, public organisations will get easier, simpler and more efficient work routines, as well as a better cooperation among employees, work processes and internal IT-systems. On the other hand, the external aim is to establish an administrative digital foundation in cooperation with citizens, businesses and other authorities. This external aim involves a strong focus on standardisation with regard to communication and the exchange of information, cases and documents. This project however does not involve standards for authenticated electronic documents.

9.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

The Single Point of Contact (»Kvikskranken«) will be build as a part of Virk.dk with a phone-service with direct access to personal counselling. It is also likely to accept questions etc. via e-mail and possibly a web-contact-form. The information as well as counselling will be available in English. Elements such

as response time requirements, use of specific languages (other than English), and liability have not yet been reviewed.

9.4 Assessment – Plans, progress and proposals for further harmonisation

9.4.1 Current plans and progress in the implementation of the Services Directive

As shown in the overview above, Denmark already has an advanced infrastructure in place that can be leveraged for the implementation of the Services Directive, in the form of the Point of Single Contact (»Kvikskranke«). The requirements under the Service Directive is to a large extent available for Danish businesses under, in particular, Virk.dk which will serve as a role-model for the Danish Single Point of Contact.

With regard to authenticated electronic documents, Danish experience is limited (if such experience exists at all). Denmark tends to have a relaxed attitude towards electronic documents, and thus already to a large extent accepts inter alia PDF document sent by unsigned e-mails. The Danish taskforce will follow the development concerning requirements and development in this area in EU, but is not likely to be an early-adopter of any technology concerning authenticated electronic documents.

Suggestions for further European support initiatives

The Services Directive and the establishment of Single Points of Contact is a valuable asset for the Internal Market. Electronic documents may play an important role in this context. However, it is important to note that a number of electronic registers may serve similar purposes as validation for specific attributes. It is thus important to consider whether it is possible to utilise systems like the one concerning the verification of VAT numbers in the Internal Market. On-line access to registers may in a number of situations be more effective than authenticated electronic document.

Possible concerns regarding the wide use of non-authenticated documents in Denmark may be considered problematic in relation to the validity of documents. However, this concern also exists in relation to analogue documentation. Authenticated electronic documents may be a solution, but registers with on-line access have the benefit that the information may be changed rapidly by the issuer. The electronic document does not necessarily have the same feature. If it does, it requires a verification in a database (as the register with on-line access).

Under all circumstances the European initiative should be careful not to impose too strict requirements to electronic documents as this may hamper the objective of securing free flow of services in the Internal Market.

In most situations those people who rely on electronic documents may not be interested in who issued the document, but rather whether the person or business has the stated qualifications, authorisations etc.
10 Estonia

10.1 General framework for electronic documents in eGovernment applications

10.1.1 Electronic documents in eGovernment applications

The Estonian eGovernment applications make extensive use of electronic documents. The 3 most important components of the eGovernment infrastructure are the national Public Key Infrastructure (PKI) and the PKI-enabled ID card; a secure data exchange system called "X-Road"; and a point of single contact: the www.eesti.ee web portal for citizens, entrepreneurs and officials. In order to understand the Estonian eGovernment solution of handling electronic documents these components need to be elaborated.

The general legal framework includes inter alia the Digital Signatures Act (the DSA); the Public Information Act and the Identity Documents Act and several regulations issued by the Government or Ministers. There is no one separate legal act to regulate eGovernment as such.

According to the Identity Documents Act, possessing an ID-card is mandatory for all Estonian residents and also for all aliens who reside permanently in Estonia on the basis of a valid residence permit with a period of validity of at least one year. Currently there are over 1 million active ID-cards (Estonia has a population of about 1.3 million).

Each issued ID-card contains two certificates: one for authentication and one for digital signing. There are also two associated private keys, protected by two separate PIN codes, on the card. The certificates contain no restrictions of use: they are by nature universal and meant to be used in any form of communications, whether between private persons, organizations or the card holder and government. Certificates on the ID-card are “Qualified” in terms of Directive 1999/93/EC.131

The X-Road acts as a backbone for all eGovernment applications. Launched in December 2001, the X-Road (X-Tee in Estonian) is a middle-tier data exchange layer enabling government databases and information systems to securely communicate with each other. It was initially developed as an environment facilitating the formulation of queries to different databases in a standardised way. The system allows officials, as well as legal and natural persons, to search data from national databases over the Internet within the limits of their authority, using a unified user interface. In addition, the system has been further developed to enable the creation of eServices capable of simultaneously using data held in different databases. Several extensions have thus been developed for the X-Road system. These include: writing operations to databases, transmitting huge data sets between...

information systems, performing successive search operations of data in different data sheets, providing services via web portals, etc. As a result, X-Road is one of the cornerstones of the Estonian State Information System.\footnote{132 eGovernment Factsheet - Estonia - National Infrastructure. Available electronically: http://www.eppractice.eu/document/3332 last accessed 02.12.2008}

The State Portal \texttt{www.eesti.ee} as a point of single contact provides a safe Internet environment for communication with the state – offering reliable information (the information is obtained securely via X-Road – the system guarantees the authenticity and integrity of the information/documents) and e-solutions for citizens, entrepreneurs and officials.\footnote{133 See: http://www.eesti.ee}\footnote{134 http://www.ria.ee/27311 last accessed 02.12.2008.} Through authentication via the national ID-card, Mobile-ID (Mobile phone with PKI-enabled SIM-card) or via electronic banking (this option will be gradually discontinued), this environment offers all users the possibility to fill in and submit electronic forms, to perform transactions with municipal and Government bodies, to access their personal data on X-Road, to sign documents digitally etc.

Entrepreneurs using the portal are additionally authorized on the basis of data in the State Commercial Register, which enables them to access additional X-road services, targeted to entrepreneurs.\footnote{134 http://www.ria.ee/27311 last accessed 02.12.2008.} Currently the State Commercial Register has its own separate web portal for entrepreneurs called the Company Registration Portal (https://ettevotjaportaal.rik.ee), which will be discussed below. The State Portal currently offers only a hyperlink to the Company Registration Portal. The State Portal is available in Estonian, Russian and English.

There are several regulations in place that regulate the requirements that the electronic documents issued by or presented to the administration have to meet. Electronic documents can be communicated between service providers and the administration either as digitally signed documents (for information on the Estonian common digital signing system see below) or through the \texttt{www.eesti.ee} state portal (utilizing X-Road - e.g. displaying of information from a state database). For the purposes of this Study the above differentiation is important because the legal and technical requirements are different. Any information or document exchanged/viewed within the PSC (\texttt{www.eesti.ee}) or X-Road environment does not need to be digitally signed because it is conveyed in a secure environment, however if electronic documents are to be issued or presented outside of the SPC/X-Road (e.g. sent as an email or attached document) then such documents need to be digitally signed in order to have legal power.

The public sector has an obligation to accept digitally signed documents. A digital signature has the same legal consequences as a hand-written signature if these consequences are not restricted by law and provided that the digital signature complies with the requirements of the DSA. The DSA stipulates that a digital signature and the system of using the digital signature must enable unique identification of the person in whose name the signature is given; enable determination of the time at which the signature is given; and link the digital signature to data in such a manner that any subsequent change of the data or the meaning thereof is detectable.
For legally binding digital signatures, time is an extremely important factor. Thus, there is a need for a time-stamping and validity confirmation service which binds the signature, time and certificate validity.

AS Sertifitseerimiskeskus\(^{135}\) (SK) chose to base its time-stamping implementation on standard OCSP. The protocol contains a Nonce field, which protects against replay attacks. Instead of cryptographically random data, the Nonce field is set to contain the hash of the data to be signed, because it can also be interpreted as just a random number. According to RFC 2560, the OCSP responder signs its response which in SK-s case, contains the original nonce (document hash), response providing/signing time and ID of the certificate used to give the signature, binding the three pieces of data together and providing the validity confirmation for the digital signature. SK stores the signed response in its log as evidence material. SK has implemented all of the above, including both client and server parts, in its DigiDoc digital signature architecture described below.

In 2002, SK together with its partners created an all-around digital signature architecture dubbed DigiDoc, which is the common digital signing system in Estonia. As the name suggests, DigiDoc aims to meet all the needs users might have about digital signature creation, handling and verification.

On the server side, DigiDoc provides an RFC 2560 compliant OCSP server, operating directly off the CA master certificate database and providing validity confirmations to certificates and signatures. On the client side, it provides a number of components.

The most important component is digital document format, which is key to common digital signature implementation and practice. SK originally based the DigiDoc document format on XML-DSIG standard. However, this had several shortcomings such as allowing only one signature per document, and in February 2002, ETSI published its extensions to XML-DSIG as ETSI TS 101 903, also known as XAdES. DigiDoc document format is a profile of XAdES, containing a subset of its proposed extensions.

Based on the document format, a library was developed in C language which binds together the following:

- DigiDoc document format
- SK-s OCSP validation service
- Interfacing with the user's ID-card using Windows' native CSP interface or cross-platform PKCS#11.\(^{136}\)

\(^{135}\) The core function of AS Sertifitseerimiskeskus (SK) is to ensure the reliability and integrity of the electronic infrastructure behind the Estonian ID-card project. SK functions as a CA (SK is Estonia's primary Certification Authority), provides certificates to the ID-card and the services necessary for utilizing the certificates and giving legally binding digital signatures. SK also functions as a competence center for ID-card and spread the knowledge necessary for creating electronic applications to the card. Established in February 2001 by two leading Estonian banks Hansapank (member of the Swedbank group) and SEB (member of SEB Group) and two telecom companies, Elion and EMT (members of the TeliaSonera group), SK has the backing of Estonian and Nordic financial and telecom sector. (See: [http://www.sk.ee](http://www.sk.ee))

The technical attributes of the DigiDoc document are regulated through “soft law”. DigiDoc document format (DIGIDOC-XML) has the following important features:

- Can be verified offline without any additional information;
- Signature can be given to several original documents at the same time;
- Protection against format attacks – type of signed document is also signed;
- Original document can be in the container or stored separately;
- Original document can be XML or any binary file (Word, Excel, PDF, RTF etc);
- Zero, one or more signatures per container;
- One validity confirmation per signature.\(^{137}\)

The Estonian IT Interoperability Framework (http://www.riso.ee/et/koosvoime/raamistik2_0.pdf – in Estonian; http://www.riso.ee/en/files/framework_2005.pdf an abridged version in English) sets out rules and principles to be followed in the development of public sector information systems. So far, two versions of the framework have been elaborated. The elaboration of the framework is led by the Department of State Information Systems of the Ministry of Economic Affairs and Communications and the document is drafted in co-operation with experts representing the public, private and third sectors. The IT Interoperability Framework and the related documents are mandatory in order to ensure mutual communication between the information systems of central and local government agencies. The framework documents cannot, however, be regarded as legal acts. Their obligatory nature is expressed through the following aspects:

- The framework and the related documents have undergone a consultation period during which central and local government agencies, the private sector, third sector organizations, as well as private persons had the opportunity to submit their proposals.
- Pursuant to the Government of the Republic Act, the Public Information Act and The Basic Principles of Estonian Information Policy, the co-ordination of the development of state information systems is assigned to the Ministry of Economic Affairs and Communications. The IT Interoperability Framework and the related documents constitute one of the tools for the development and co-ordination of the state information system.\(^{138}\)

Some support systems described in the framework have recently been regulated by Government regulations – these include the classifications system\(^ {139}\), the system of address details\(^ {140}\), the data exchange layer for information systems – X-Road\(^ {141}\), the geodetic system\(^ {142}\), the system of security


\(^{139}\) https://www.riigiteataja.ee/ert/act.jsp?id=12910889 (In Estonian)

\(^{140}\) https://www.riigiteataja.ee/ert/act.jsp?id=12901083 (In Estonian)

\(^{141}\) https://www.riigiteataja.ee/ert/act.jsp?id=12956835 (In Estonian)
measures for information systems\textsuperscript{143}. The sixth support system is the administration system for the state information system\textsuperscript{144} (RIHA). The objective of RIHA is to ensure transparent administration of the state information system, plan for the state information administration and support the interoperability of databases that provide public services\textsuperscript{145}.

Currently a third version of the Estonian IT Interoperability Framework is being prepared however this is not yet available to the public.

10.1.2 Electronic documents for the purposes of the implementation of the Services Directive

There are no specific plans or policies targeted directly at the implementation of Article 8 of Directive 2006/123/EC. However, the implementation of the Directive will be achieved, because the necessary advanced IT infrastructure and solutions have been developed and are already operating at the national level. The cross-border conveyance of electronic documents/information should work similarly as was described above – either as digitally signed documents/emails or via secure web portals, which act as points of single contact. Electronic ID-cards issued by some Member States can already be used in the Company Registration Portal for authentication and for giving digital signatures. Currently the electronic ID-cards of Portugal, Belgium and Finland and the Lithuanian mobile-ID can be used to gain access and sign documents digitally in the Company Registration Portal. According to some sources the recognised foreign eID cards should soon be supported also in the \url{www.eesti.ee} portal.

The DSA regulates the recognition of certificates issued by foreign certification service providers and of digital signatures created on the basis thereof. Certificates issued by a foreign certification service provider are recognised as equivalent to certificates issued by certification service providers acting on the basis of DSA if at least one of the following conditions is met:

1) according to a case-by-case decision of the Ministry of Economic Affairs and Communications, the foreign certification service provider complies with the requirements provided for in the DSA and legislation established on the basis thereof; or

2) the certificates of the foreign certification provider are guaranteed by a certification service provider acting on the basis of the DSA who assumes responsibility for the accuracy of the data contained in the certificates; or

3) the certificates issued by the foreign certification service provider are recognised by an international agreement entered into by the Republic of Estonia.

\textsuperscript{142} \url{https://www.riigiteataja.ee/ert/act.jsp?id=12987975} (In Estonian)
\textsuperscript{143} \url{https://www.riigiteataja.ee/ert/act.jsp?id=12901110} (In Estonian)
\textsuperscript{144} \url{https://www.riigiteataja.ee/ert/act.jsp?id=12933746} (In Estonian)
Thus, there are several options on how foreign electronic ID cards may become officially recognised in Estonia, however the biggest challenge will be the cross-border interoperability of the IT systems.

When deciding whether the foreign certification service provider complies with the requirements provided for in the DSA and legislation established on the basis thereof, the Ministry of Economic Affairs and Communications follows the principle that the foreign CSP-s and certificates are at least as secure as the Estonian ID-card. This method is not perfect because the variations in the legislation of Member States make objective comparisons difficult, and more general well defined criteria should be taken as a basis. Therefore the Ministry of Economic Affairs and Communications evaluates three key elements:

1) Whether the certificates are Qualified Certificates in the sense of Directive 1999/93/EC;
2) Whether the CSP is a dedicated government organisation or an accredited institution in a contractual relationship with the state;
3) Whether the device that contains the private key is a Secure Signature Creation Device in the sense of Directive 1999/93/EC.¹⁴⁶

More specifically in the sense of the Services Directive the cross-border establishment of companies is already possible as a one-stop-process via the Company Registration Portal. The only limitation is the interoperability and the recognition of the eID solutions of different Member States as there is no EU-wide body to coordinate the process and the recognition process and overcoming the interoperability issues may prove cumbersome.

10.2 Specific document types

10.2.1 Extracts from commercial registers

Electronic documents are commonly used and available in Estonia. The commercial registry extracts are a key example of this. The use of electronic commercial registry extracts is administered by the Centre of Registers and Information Systems (RIK). RIK develops and administers several registers and information services. These include the Commercial Register, E-notary, Land Register and several information systems for law and criminal jurisdiction (court information system, E-file, E-justice etc.) which are all linked to the X-Road.

The electronic Commercial Register has two main functions:

1. It serves as an information system for obtaining the information on legal entities registered in Estonia;

The Central Commercial Register\textsuperscript{147} is an on-line service based on the central database of registration departments of the courts. This central database includes digital data from the commercial register (for all legal entities), the register of non-profit associations and foundations and the commercial pledge register.

The basic information concerning the abovementioned entities (which is freely searchable for any Estonian or other national on-line at \url{https://ariregister.rik.ee/index.py?lang=eng}) includes:

- the business name (valid data and history),
- registration code,
- the date of the first entry to the register,
- the status, the location area (valid data and history),
- the address, the share capital (valid data and history),
- fields of activity and principal activity (valid data and history),
- members of the management board (valid data and history),
- bankruptcy trustee & liquidator (valid data and history),
- the webpage and proceedings information (valid data and history).

It is also possible to obtain information (for a fixed cost for each query) on:

- commercial pledges,
- members of the supervisory board (valid data and history),
- annual reports,
- articles of association,
- basic financial information, including capital and date of deposit of balance sheets,
- means of communication,
- representation rights,
- founder (and declarative information on the shareholders).

The abovementioned information and documents that can be obtained from the register are not, however, certified. Thus if there is a need for a certified document, a paper version has to be ordered from the Commercial Register.

This situation is expected to change once the amendments of the DSA are approved and extracts from the commercial register can be digitally stamped.

2) It enables the foundation of and registry changes to a company\textsuperscript{148} on-line though the Company Registration Portal.

Company Registration Portal (the CRP available at \url{https://ettevotjaportaal.rik.ee/?chlang=eng}) is a portal for the entrepreneurs to communicate with the registration departments of the courts and the central Commercial Register to perform different acts in the register. Entrepreneurs can submit an application for an entry of changes to the register in two ways:

\textsuperscript{147} Please see \url{http://www.rik.ee/33169}.

\textsuperscript{148} Private limited company, sole proprietor, limited partnership, general partnership or non-profit organization.
by logging into the CRP using an authentication method described above (including access with an Estonian, Portuguese, Finnish or Belgian ID-Card; Estonian or Lithuanian Mobile-ID); or

• by digitally signing a document with DigiDoc and sending it to the registrar (assistant judge at the Commercial Register).

In addition to filing changes to the Commercial Register, it is also possible to perform the following actions in the above described method, which do not constitute entries; however they are of declarative value:

• submit a list of the members of supervisory board with their personal data and changes in it,
• submit a list of auditors with their personal data and changes in it,
• submit telecommunications numbers,
• submit information about changes in the area of activity and submit annual reports.

Estonia is also a member of the European Business Register\textsuperscript{149}, which aims at interlinking European business registers, which would eliminate the need for exchanging extracts.

10.2.2 Criminal records

In Estonia digital extract from punishment register can be obtained. Under the Punishment Register Act (\textit{Karistusregistri seadus}) the criminal record consists of electronic registry cards. The Punishment Register Act regulates the proceedings how to manage specified data about natural or legal persons and also sets the general principles of maintenance of the punishment register. Any person is entitled to get information from the Punishment register (criminal register) regarding data about him/herself. Company owners or members of the management board are entitled to apply for the criminal record of the relevant legal person. The holder of the Punishment Register is the Police Board.

It is possible to apply for electronic extracts from the punishment register. Application to obtain the criminal record from the Punishment Register shall be filed on paper or through electronic means. The application can be obtained from the Police Board’s website (http://www.politsei.ee/?id=952) in DOC or PDF format. These can then be digitally signed and the resulting DigiDoc file can be e-mailed to the Punishment Register.

After a person has electronically requested an extract from the Punishment Register the Punishment Register official will send a digitally signed extract within 10 days. If applied only once per year the extract is free of charge but for each additional extract during that year an additional state fee of EEK 50 applies. For administrative use the Punishment Register will send the extract within one day and no state fee is required.

\textsuperscript{149} The European Business Register is a network of business registers kept by the registration authorities in most of the European countries. Please see http://www.ebr.org/.
There are plans to integrate the Punishment Register into the E-file solution. E-file allows persons to see their own criminal or misdemeanor record from one web-solution. Users must authenticate themselves using an ID-card. The purpose of the E-File information system is to provide the parties to criminal, civil, administrative and misdemeanor (court) proceedings with a comprehensive overview of different stages and operations of the proceedings as well as the decisions made. Until now law enforcement authorities have administered their procedural information separately, but the E-File will contain the entirety of the information, ensuring a comprehensive overview of the status of proceedings, operations, decisions, etc. In addition, the quality of information concerning punishment will improve.\(^{150}\) The E-file database is accessible through the X-Road solution.

### 10.2.3 Extracts from professional registers

In Estonia professional registers are not common and in practice professional registers are relatively new. The Estonian Qualification Authority is managed by a private entity but the organisation is controlled by the Estonian government. This authority was established in 2001. The professional register it maintains is public and everyone can check the register or find the information through X-Road.

Generally there is no official plan to make the issuing of electronic documents by the professional registries mandatory. However, the state encourages different registers to be attached with X-Road solution.

### 10.2.4 Certificates of insurance

In the sense of electronic documents used by the insurance sector the common practice is to sign the insurance contract with digital signature and then the insurer sends the certificate of insurance via e-mail. Generally the certificates of insurance are issued in an electronic form however these are usually not digitally signed.

### 10.2.5 Proofs of qualifications

Proofs of qualifications are documents issued by private and public sector for which only paper originals are available. It is possible to send the proof of qualification via-email but even it is digitally signed the electronic version is not equal to the paper original. Sending digitally signed proofs of qualifications via e-mail is not common. Mainly the documents are given hand to hand in paper originals. The paper original has serial number that can be checked through an Internet database.

Registers held by the private sector are usually public and everyone is able to check if a person has or has not the qualification needed (e.g. via a respective website). It is possible to get information about

---

\(^{150}\) What is E-file? Internet access [http://www.just.ee/e-file](http://www.just.ee/e-file)
education through the X-road system but this information includes only the obtained level of education. Persons can check such information via X-Road only about themselves.

Currently, no plan exists to encourage/mandate the issuing of proofs of qualifications as an electronic document.

10.2.6 Statements from the service provider

The common solution of accepting electronic statements from service providers is via websites (PSC) or e-mail (using digital signature). Two examples – the filing of annual reports and tax declarations are discussed below.

Statements in the context of the Commercial Register should be interpreted as annual fiscal statements (annual reports) of companies. Access for submitting annual reports electronically is made possible to persons with the right of representation (board member, general partner, liquidator or trustee in bankruptcy) according to the valid entries of personal identification codes in the central database of registration departments of courts.

When submitting an annual report electronically, confirmation of one board member is enough. All the board members can confirm the annual report if they wish to do so.

If an auditor’s report is added to the annual report then the auditor must give his confirmation to the report as well. When entering the company registration portal, the auditor can search for a company by registration number when first choosing the menu of filing of annual reports and give his confirmation the same way as a board member.

If the annual report with the auditor’s report cannot be confirmed electronically by the auditor, then the auditor’s report can be submitted on paper to the registration department courts (i.e. separately from the annual report).

The submission of the abovementioned reports is carried out via the company registration portal.

Through the e-Tax Board web portal (http://www.emta.ee/?id=12223) companies (service providers) can electronically file social tax and value-added tax declarations; file requests for refunds of over-paid taxes; fill in their customs declarations, and access the balances of all taxes.
10.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

10.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

The communication between the PSC and public administrators or private organisations is based on the X-Road\(^{151}\) data exchange layer and also relevant are the Electronic Document Exchange Centre (DEC) and the Administration System of the State information system (RIHA).

The state information systems’ data transport layer X-Road is a technical and organizational environment that enables secure data transfer between digital state databases and information systems and enables secure data transfer between individuals and state institutions. It also coordinates the access of individuals to information being processed in state databases.\(^{152}\)

X-Road is a platform-independent secure standard interface between databases and information systems. A database is adapted to X-Road by setting up an Adapter Server, which contains a SOAP server and X-Road rules. Information systems need a SOAP client and understanding of X-Road rules. To secure the system, each party accesses X-Road via its Security Server. X-Road Security Server is a standard software solution that encrypts/decrypts outgoing/incoming messages, filters incoming messages as a firewall, and logs messages it receives. Traffic between Security Servers is encrypted with PKI. Security Servers have to be certified by the X-Road Certification Authority. Certificates are available for verification from X-Road Central Servers, which are duplicated. There is no redundant centralization – Security Servers create connections directly to each other. Data from Central Servers is cached in Security Servers by use of DNSSEC.\(^{153}\)

The X-Road system has been developed to enable the creation of eServices capable of simultaneously using data held in different databases.\(^{154}\) All state databases had to be interfaced to the X-Road environment by 1 June 2008\(^ {155}\) and currently about 2000 services are available via the X-Road.

---


155 https://www.riigiteataja.ee/er/act.jsp?id=12956835 (in Estonian)
Since 1 October 2008 all Ministries, State Chancellery, county governments, public offices and inspectorates have been obliged to exchange documents electronically using the Electronic Document Exchange Centre (DEC) which is linked to the X-Road.\(^{156}\)

The Document Exchange Centre (DEC) is a central information system for connecting dispersedly located records management systems via the X-Road. Its primary function is to transfer documents, in particular digitally signed documents.

There are three ways to do that:

1) If the agency has a records management system, it is connected with the DEC, which enables to send documents to the records management systems of other agencies.

2) If the agency does not have a records management system, the DEC transfers documents to that agency by e-mail.

3) Citizens can e-mail documents to the DEC to be forwarded to relevant agencies. Agencies can reply to citizens by e-mail (either directly or through the DEC).

The exchange of digital documents between records management systems through the Document Exchange Centre makes use of document forms with uniform data structure, the Extensible Markup Language recommended by the World Wide Web Consortium (W3C) and the State Chancellery’s guidelines on document elements and metadata. To guarantee the uniform presentation of document content, state agencies must co-ordinate the XML-based presentation forms of the documents to be channeled through the DEC with the State Chancellery. The coordinated XML-based presentation forms will be used for setting up a database that would allow the reuse of uniform presentation forms.\(^{157}\) For more information on the DEC visit: [http://www.ria.ee/28567](http://www.ria.ee/28567)

The objective of the Administration System of the State information system (RIHA) is to ensure the interoperability of public sector information systems and the re-use of technical, organizational and semantic resources, so as to give a clear view of the State registers and of the services provided by them.

The creation and maintenance of Government databases is governed by the Public Information Act which establishes an Administration System for State information systems (RIHA), where all the databases and information systems must be registered.

RIHA includes metadata about existing public sector databases – ranging from the information on the administrators of the databases to the eServices offered and the technical data concerning the environment/platform. Registration in RIHA is web-based; the user is authenticated and permissions are given by using the national electronic ID Card.

---

156 https://www.riigietataja.ee/ert/act.jsp?id=12869602 (In Estonian)

In the same web-based environment, requests to other information systems can be made in order to launch a new X-Road based service. RIHA additionally administers two supporting systems of State registers; the system of classificators and the address data system. The system of integrated registers enables to apply new principles of administrative arrangements: citizen-orientation, flexibility, swiftness, as well as cost and time effectiveness for both the citizen and the State.

RIHA is used to administer the X-Road and serves as a tool enabling the performance of the following activities: obtaining information about existing services, as well as those under development; applying for the right to use a service; proposing the creation of a new service; using data services; administering in-house access rights; ensuring legitimate use of data services. 158

10.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Delivering documents back to service providers by the public administration or private organisations can be achieved in several ways. The most obvious is directly obtaining the document via the PSC (e.g. on screen or by downloading) or emailing of the digitally signed documents directly to the service provider. Additionally some e-Services currently available via the State Portal (www.eesti.ee) make use of SMS technology to send notices 159 or information directly to the user’s mobile phone. SMS technology may well be applied to e-Services offered to service providers.

Draft legislation to amend the DSA is currently being processed by the Parliament of Estonia. The planned amendments will regulate the use of digital stamps – for now officials have to sign the outgoing documents with their personal ID-card and such a process takes time. Digital stamps would be analogous to digital signatures in legal and technical terms; however they would also be usable by legal entities (private and public), thus enabling the automatic generation of digitally stamped documents, which carry evidentiary value (i.e digitally stamped statement from an Internet bank; extract from the Commercial Registry’s website can be instantly digitally stamped; etc.).


159 For example high school seniors have the possibility of being notified of their state examination results via SMS.
10.4 Assessment – Plans, progress and proposals for further harmonisation

10.4.1 Current plans and progress in the implementation of the Services Directive

Estonia has had an advanced IT infrastructure in place for several years that enables the conveying of digitally signed documents and e-Services. These systems have been under constant development. In light of the Services Directive no major legal or technical challenges therefore have to be solved. The only exception is the implementing of interoperable cross-border eID solutions and information systems.

The Estonian Information Society Strategy 2013, approved by the Government of the Republic (on 30 November 2006), set as some of its most important goals inter alia that:

- citizens of other countries, especially Member States’ nationals have the opportunity to use relevant Estonian e-Services;
- all records management will be electronic;
- the national information system will be service based and user oriented rather than institutionally built up.

The lack of officially recognised pan-European CSP-s; a standardised system of agreements between the national CSP-s of Member States; or other uniform and widely recognised solutions for cooperation and interoperability of the IT systems is threatening to hinder effective and business oriented cross-border solutions for electronic document and information movement. Even the current recognition of Portuguese, Belgian and Finnish ID-cards and Lithuanian Mobile-ID by Estonia is not without compromise – the solutions used are not fully integrated. The systems are not backwards compatible, e.g. a digital signature given in an Estonian PSC using a Belgian ID-card will be using Estonian certificates, meaning that the documents are useable in Estonia but cannot be verified using Belgian solutions. This is a clear example of the lack of interoperability.

An innovative approach would be making some of the services available on X-Road accessible to information systems in other Member States thus eliminating unnecessary steps that the service provider has to take, since information can be verified via information systems directly and electronic documents as such are not needed. But the creation official information exchange gateways to the X-Road is hindered for the same reasons as stated above.

10.4.2 Suggestions for further European support initiatives

The establishing of a European authority to manage a trusted list of CSP-s that meet commonly accepted high standards seems like a viable option to develop a fully functional cross-border solution to electronic document delivery and integration of information systems. There are of course several legal and technical obstacles that have to be solved in order to achieve this. The technical side of integrating the Estonian IT infrastructure to cross-border solutions is not a major issue since common and open standards are used. The legal aspect is more serious because the authentication of the users and the validity of the digital signatures have to meet very high standards set by the DSA before any integration or creation of cross-border solutions can take place.
11 Finland

11.1 General framework for electronic documents in eGovernment applications

11.1.1 Electronic documents in eGovernment applications

At the national level, Finland does not have a generic framework related to electronic documents in eGovernment applications in general. A number of eGovernment applications from government and provincial entities are available to citizens and enterprises, but they are regulated and implemented on agency or domain basis, and in paper form. The vast majority of the most used services that fall under the scope of the Service Directive are handled on the local government (province) level and not the national, although only national level efforts are currently undergoing in order to implement the Service Directive Art. 8 requirements for single-points of contact. The main single-point of contact service provided in Finland is the EnterpriseFinland.fi portal service.

Finnish public services rely on electronic documents only for a small minority of services, either in the form of files that need to be presented by the end user to the application; or in the form of files that are issued to the end user after the conclusion of a transaction. The Finnish approach to eGovernment revolves largely around trusted web services and around establishing trusted relationships between public administrations and private sector organisations for the direct exchange of authentic information. For information exchange, trusted networks are used instead of requiring the creation of a specific electronic document. Often service providers may be able to download electronic forms and applications or demand paper based documents via an electronic channel, but the transactions are electronic only at a initial level and paper based submitting and reception of documents is the rule.

With regards to electronic documents, no generic legal framework or technical requirements exist. Electronic documents currently in common use in public administrations are mainly downloadable Microsoft Word documents or Adobe PDF documents. The Finnish eGovernment approach relies on two key elements: service integration for electronic authentic sources, such as the Population Information System\(^\text{161}\), the Business Information System\(^\text{162}\) and the National Board of Patents and Registration\(^\text{163}\), and offering multilingual access to services using electronic authentic sources. The Business Information database contains authentic administrative data of every economically active entity (registered to the Finnish Tax Administration, Trade Register or Register of Foundations) established in Finland whereas the Population Information System contains basic information about Finnish citizens and foreign citizens residing permanently in Finland, about buildings, construction projects, residences and real estate. As the examples further below will show, the Finnish eGovernment strategy revolves around ensuring that these authentic databases contain all required information, and in making these resources accessible to service providers which have a need to access and use the services and information.

---


\(^{162}\) See [http://www.ytj.fi/english/](http://www.ytj.fi/english/)

From a technical perspective, governmental services largely exchange data through closed networks. Several services have been implemented in a generic electronic portal called EnterpriseFinland.fi\textsuperscript{164} which offers access to the main web services offered by the government to service providers. These web services consist mainly of giving advice to service providers, providing links to relevant electronic forms and online services, where registered users (in the private sector) are able submit statutory and mandatory filings using certain authentic resources, including e.g. insurance and tax information. Many electronic document services are related to fulfilment of mandatory requirements which involve information exchange with private organisations (namely insurances and pensions) and public services, which affects the implementation of the Services Directive, as will be discussed further below.

Electronic documents are not generally issued to services providers or end users or requested from them in the context of eGovernment applications, and this is unlikely to change in the near future. From a Finnish perspective, documents as a whole often constitute an unnecessary intermediate step that can be eliminated from public processes by correctly leveraging electronic resources. The introduction of electronic documents to replace paper ones would then not be an optimal step forward in facilitating the life of end users or in improving administrative efficiency, which regards process re-engineering as a key target for electronic service development in the future.

11.1.2 Electronic documents for the purposes of the implementation of the Services Directive

Within the context of the Services Directive, internally electronic documents are not used. There are however some services where service providers can provide electronic documentation and where documents are handled electronically, and where documents carry some sort of electronic signatures. In order to understand the Finnish situation, it is necessary to first examine how service providers are currently integrated within the electronic service chains.

As noted above, any economically active entity in Finland must be registered in the Business Information System. The BIS offers a single-point of contact for providing mandatory filings of other business related formalities (e.g. VAT registration and filings, mandatory pensions insurance and social security payment filing obligations). However even though the BIS contains administrative role descriptions that are used within the framework of identity authorisation in the tax filings service, demonstrating technical capability through diplomas, obtaining licenses and permits, registering with professional bodies, etc. are not part of the BIS services. In order to assist entrepreneurs in meeting all formalities, different internet services have been put in place. A central hub, or web portal collecting links for all business related services has been developed by the Ministry of Employment and the Economy under the domain EnterpriseFinland.fi, which exists in Finnish, Swedish and English. Enterprises mainly access mandatory filings services from a range of private online services.

The main privately managed online filing services are the collection of so called TYVI –services and Pensions Insurance eServices. TYVI services are a system enabling companies to transfer tax return information electronically to the tax authorities. Businesses can transmit e.g. tax and information

\textsuperscript{164} See http://www.yrityssuomi.fi/default.aspx?nodeid=15356
returns, Annual Notifications, Monthly Tax Returns, and Income Tax Returns of corporate taxpayers. In addition, they can use the services to request and receive employees’ withholding tax information separately for each individual employee. The TYVI Service Providers are private companies that run the service on behalf of the tax administration. These service providers are authorised to maintain information in the tax system and other relevant authentic sources, but as the organisation filing the information is responsible the content of the data, the TYVI service providers’ role is focused on service delivery and accessibility, and not to the information content as such.

Currently there are 4 TYVI -service providers and each service provider offers different service packages for service users. The electronic services offered through the TYVI services are designed for all types of businesses and organisations, but for smaller organisations, they are mostly used by intermediaries that provide outsourced financial and accounting services. This delegation of tasks is possible due to the federated identity service offered by the tax authorities. As electronic filing is done within a trusted environment and after positive authentication and authorisation, no further signing of electronic documents or signing of paper forms are necessary. The services require, depending on service provider, client software installations, system integration or simple web browser access.

The EnterpriseFinland.fi portal is under further development and a telephone based assistance service is scheduled start for 2009. The portal will then function as a gateway between service providers and different professional organisations that they may need to communicate with. The traditional role of assisting service providers corresponds closely to the tasks that the Services Directive foresees for the single-points of contact. Nevertheless as the single-point of contact should be able to offer their services entirely electronically, this requirement will not be fulfilled by the portal in the foreseeable near future.

The Finnish government is developing several electronic service platforms for electronic content and document management, identity federation services and service delivery between and across different administrations, which are essential for building the necessary infrastructure for single-points of contact. In addition, a citizen and business service account platform is under development, which would act as single-point of contact for all government services. Nevertheless these services will not fall under the scope of the Service Directive Art. 8 and only the EnterpriseFinland.fi portal can be regarded as the centre-piece for implementing the Services Directive in Finland.

---

165 See http://www.vero.fi/default.asp?language=ENG&domain=VERO_ENGLISH
166 See http://www.vero.fi/default.asp?language=ENG&domain=VERO_ENGLISH
167 So called VALDA project, see www.vm.fi/valda
168 So called VIRTU project, see http://www.vm.fi/vm/fl/13_hallinnon_kehittaminen/05_it_toiminta/01_valtit/03_yhteiset_tietojarjestelmat/02_VIRTU/index.jsp
169 So called “Asiantuntija” project, see http://www.vm.fi/vm/fl/13_hallinnon_kehittaminen/05_it_toiminta/01_valtit/01_sahkoinen_asiointi/02_asiointitili/index.jsp
170 So called “Asiointitili” project, see previous
As the Directive allows multiple single-points of contact to be established, it is envisaged that each of the services linked in the current portal will continue to evolve on an agency or domain basis, and the portal service will continue to offer only centralised information on the existing services and hyperlinks to the single-points of contact services. This tendency is enforced by the fact that many of the most heavily used services are not provided on the central government level, but are relevant to provincial level local government bodies. New legislative changes that are coming into force in 2010 will affect service provisioning on the province level. From a legal point of view, this will facilitate electronic exchange of data between administrations, but these changes will not directly affect how the provisions of single-points of contact offering electronic services will be met.

There are no concrete plans as to the implementation of the Services Directive in Finland. Until now, Finland has focused on finalising the required screening exercises. In the government, emphasis has been placed on following the Directive's requirements for administrative simplification, but also placing a lot of interest in issues not covered by the Directive, namely that of multi-lingual service provisioning, which is seen as a key element for online services in general.

As was to be expected, the screening exercise thus far has shown that electronic documents are only very rarely used in practice, both by public administrations and by private organisations, and that use of electronic documents was unlikely to take off in the near future.

By the end of 2010 and during 2011 some of the key infrastructures for data exchange and identity federation between administrations will be set up, which will make the implementation of single-points of contact and use of electronic documents a more tangible reality. For 2009 a new amendment is also planned for the law on Electronic Signatures. The amendment would include legislation on strong authentication and provisioning of electronic authentication and identity services for the public, businesses and the government. The amendment text is under preparation and it is intended to bring support for the implementation of the Service Directive Art. 8. In many regards, the problems related to strong authentication of users and identity federation for public servants has been seen as a major obstacle for the creation of single-points of contact in Finland.

As an example, the tax authorities have built an identity federation service linking user roles (provided by the National Board of Patents and Registration role-information service) with user identity information (provided by the Population Registry system), and using either bank service ID tokens or national eID for initial signup for “Katso” credentials. This service has several technical advantages for registering authorisations for service providers, but it also has drawbacks related to legal provisions that should be dealt with new legislation. Identity federation in the service scheme offered by the tax authorities is based on Liberty Alliance and the use of a network of trust, which is also

---

171 See p.19 of the Handbook for the implementation of the Services Directive offered by DG Markt: “The concept of “points of single contact” does not mean that Member States have to set up one single centralised body in their territory. Member States may decide to have several “points of single contact” within their territory. The “point of single contact” must however be “single” from the individual provider’s perspective (i.e. the service provider should be able to complete all procedures by using only one such point of contact).”

172 Ministry of Labour and the Economy report from 19.11.2008: “Palveludirektiivin implementointiin liittyvien sähköisten asiointipalvelujen selvittäminen”.

173 The so called “Katso” service, see: http://www.vero.fi/katso_etusivu/?language=ENG
envisioned in the general identity federation scheme for public servants (the VIRTU project). Technically the services can be accessed cross-border on a Pan-European level, but obstacles remains with regards to user role provisioning and credential validation on a cross-border level.

In relation to specific electronic documents to be provided by service providers (i.e. in cases where administrative simplification has not resulted in the elimination of the need for original documentation), it is not yet certain what approach will be followed, either with regard to signatures or with regard to documents.

For Finnish service providers, the approach is likely to focus on using the signature capabilities of Finnish eID certificates either on a smart card or as a mobile service, or use of alternative techniques to circumvent the use of electronic signature objects, as the take-up for the certificate based eID’s has not been satisfactory. For service providers of other Member States, the Finnish administrations is currently examining how they can incorporate trusted lists of CSPs into their solutions. However, the Finnish authorities have no concrete plans or initiatives addressing this issue.

With regard to signature level requirements, while the Finnish signature is considered to be a qualified signature, it has not yet been decided whether this will also be required of electronic signatures in the cross border context, or whether there will be a requirement for qualified signatures at all. In the Finnish legal context, a legal act can be recorded by a number of means, and a qualified digital signature does not necessarily result in a stronger legal value than other means. This makes it possible that electronic documents may be recorded as having legal effect without applying a formal qualified electronic signature to the document. The Finnish government is constantly looking at the direction in which European initiatives are evolving to determine how they can mitigate the use of qualified electronic signatures and how they would be able to integrate an optimal number of e-signatures from other Member States.

Regarding the document types to be supported, Finland is similarly awaiting what trends are emerging at the national level in other Member States. Finnish eGovernment applications use Microsoft Word documents, Adobe files and XML forms for communicating with users and internally these same products will eventually be used for the implementation of the Services Directive. The ongoing development project on document content management and digital archiving VALDA \(^{174}\) will address the issue of electronic documents for internal processes, but so far no technical specifications have been issued with regards to technical formats for documents or electronic signatures. Generally speaking, Finnish administrations do not require the use of electronic documents from the end users, and other communications means are also accepted, such as free-form electronic mail, and thus a large margin of flexibility still remains in making implementation choices. If interoperability would require the uptake of a specific standard, it would likely be possible to integrate this, provided that the standard is sufficiently supported at the international level, and does not enter into direct conflict with the tradition of open and accessible government.

From a practical perspective, service providers wishing to become economically active in Finland using electronic means, have the possibility to hook up at the EnterpriseFinland.fi portal, which functions as a single-point of contact and as information collection of other relevant single-points of contact. The portal provides businesses with relevant information and offers links to relatively limited, low-tech and accessible services, such as on-line web forms for data entry and generic e-mail or

\(^{174}\) See [http://www.vm.fi/valda](http://www.vm.fi/valda)
paper mail for transmitting specific documents through an array of existing eService portals such as Suomi.fi\textsuperscript{175}. As mentioned above, the Finnish administration has not yet made clear decisions, plans or strategies on which document types and signature requirements will be imposed. These issues depend to a large extent on the evolutions at the European level. The EnterpriseFinland.fi portal will not be responsible for ensuring the proper follow-up, including by interacting with any competent administrations or private organisations, but only for providing information and links to the proper administrations.

From a citizen or private user point of view, an e-payment module exists within the VETUMA authentication service\textsuperscript{176}, which is used as a generic login service for several public online services both on the national and local levels. The electronic payments module supports international payment cards from Visa and MasterCard, and therefore the Finnish authorities sees that it can be used also for providing certain fee-based services on a cross-border level. As a backdrop, it might be interesting to note that the Finnish authorities have been investigating the possibility to take advantage of the proprietary identification schemes offered by international payment services (such as Verified by Visa for example), but these have been seen as problematic from the point of view of liability, scheme ownership, commercial proprietary rights and interoperability issues with standards based identity services provided by national authorities and other European countries.

### 11.2 Specific document types

#### 11.2.1 Extracts from commercial registers

Electronic documents are not used by the Finnish administrations, and the re-use of authentic sources is much favoured. The Business Information System gives an example of this, as it offers an electronic view over the Internet to the business information but provides only paper form printed documents containing the same information. A user may make an electronic copy of the online information, but this does not constitute an official document, nevertheless administrations would have to consider this form of unofficial document also as having validity.

All key information related to economically active independent entities in Finland is collected by the BIS, as noted above, and it acts as the collection point for all commercial register information in Finland. The information itself are stored in different locations and under different administrations. Basic information about all business entities collected by and represented in the BIS includes:

1. Latest information and as of date for:

\textsuperscript{175} Suomi.fi is the national portal service that thrives to collect all different eServices available in Finland. It provides a number of online forms and applications from different services as well as advise on and links to other topical eServices. See [http://www.suomi.fi/suomifi/english/index.html](http://www.suomi.fi/suomifi/english/index.html)

\textsuperscript{176} See [www.suomi.fi/vetuma](http://www.suomi.fi/vetuma) in Finnish and [http://www.suomi.fi/suomifi/qualitytotheweb/eservices_and_forms/eservices/vetuma_service/vetuma_service/VETUMA_service.pdf](http://www.suomi.fi/suomifi/qualitytotheweb/eservices_and_forms/eservices/vetuma_service/vetuma_service/VETUMA_service.pdf) for English overview
2. Information on the source of the data:

- National Board of Patents and Registration of Finland
- Tax Administration
- Common (usually means the Population Register System)

3. Information on registrations in force (registered / not registered), name of register, status information and as of date for:

- Trade register
- Tax Administration
- Prepayment register
- Value added tax-liability
- Employer register

4. Information on prepayment registration validity, events, dates, next revision dates and Business ID history

All of this information is publicly accessible and freely searchable online\(^{177}\). As noted earlier, the information does not constitute an official document, therefore a company that needs to claim the information for use in e.g. a public tendering process, will need to apply for official extracts in paper form. Electronic documents do not exist at this time, nor are there any plans for the future on this matter. The free BIS information service is meant for checking information concerning individual businesses and not for providing official documents in electronic form. The use of the BIS is done anonymously and therefore use of search robots is forbidden. Also the maximum amount of searches from one IP address is limited to one thousand during one day. Mass-scale information service based on the information contents of the BIS is offered by several private enterprises which offer additional services such as e.g. payment record and history information.

The National Board of Patents and Registration of Finland is a partner in the European Business Register which strives to make it possible to obtain comparable, official company information from the countries connected to the network.
11.2.2 Criminal records

Extracts from the criminal register exist in Finland only in a paper format. An application for the extract can be obtained through the links provided in the EnterpriseFinland.fi portal, although one needs to go through the full index to find the service. The criminal records are a national central register where data mostly on those sentenced to imprisonment are recorded. Data is gathered and stored as well as submitted for the imposition and execution of penal sanctions. The information is provided by the Legal Register Centre\(^{178}\), which is an agency under the Ministry of Justice.

Requests for the extract can be made partly electronically using the available PDF forms. The resulting document is printed and delivered by traditional mail in a paper format. Electronic requesting is not envisaged and use of electronically signed PDF extracts will not become commonplace in the near future.

A private person can be granted an extract on herself for a visa, work permit, residence permit, or some other equivalent reason. The extract can be ordered with a free-form application or by using a readymade form. The application can be sent by mail, fax or e-mail, but if the client wants to obtain the extract personally from the Legal Register Centre, she will have to prove her identity. There is a recommendation that the applicant should sign the application form, but even if an application is sent by e-mail without a signature, it will be accepted if it contains the applicant's contact data and there is no reason to suspect its authenticity and integrity. It is a usual practise within Finnish administration not to require signatures on applications, nor to set formal requirements for applications relevant to private persons. As a privacy safeguard, the Finnish law does not authorise private organisations to apply for a person's criminal record, and the person cannot authorize e.g. her employer to order the extract. In practise, there are no technical safeguards in place to enforce this.

11.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations, orders or stakeholder bodies. While it is difficult to obtain a complete overview, it does not appear that the extracts issued by such private organisations are commonly issued in an electronic form. The Ministry of Education has competence in the field of controlling professions requiring specific certification, accreditation or permit, but professional registers are managed by separate entities. These entities communicate using authentic source repositories and avoid using specific documents except for printed certificates.

Currently, no plans exist to make the use of electronic documents mandatory or to encourage them further. The Finnish BIS provides an interface for a business role service, which states the “professional qualification” of the service provider, attesting to its acceptance to offer the covered services in Finland. The role information is provided in real time from the Finnish Chamber of

\(^{178}\) See http://www.oikeus.fi/oikeusrekisterikeskus/18593.htm
Commerce and with an information service from the National Board of Patents and Registration. This is a subscriber service with request fee.

For professions requiring special permit, such as healthcare professionals, similar services exist through the “Terhikki” medical professional information repository service179, which is accessible to all healthcare organizations using a simple LDAP interface. Again, there seems to be little added value in issuing separate documents attesting role, position or qualifications information.

### 11.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form, unless online printouts are considered as electronic documents. The types of insurance certificates service providers need to request are statutory pensions and other employer and employee insurance certificates180. The certificates are required e.g. when participating in a public tendering process. The certificates only attest to the orderly payments made towards statutory insurance policies.

While it would be legally possible to provide insurance certificates in an electronic form under the terms of the Finnish eSignatures Act, in practice this issue has not received any particular attention since it affects namely the domain of eTendering, which is dealt with in other contexts.

Currently, no plans exist to make the use of electronic certificates of insurance mandatory or to encourage them further. For the purposes of Finnish single-points of contact, the emphasis is mostly on ensuring that original documents are no longer requested unless this is absolutely necessary, in compliance with the administrative simplification obligations of the Directive.

### 11.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications: generally, these are private sector issued documents for which only paper originals are available. While electronic copies might occasionally be presented in the form of unsigned scans, this is merely a matter of convenience. No specific rules or framework exist for electronic proofs of qualification beyond the general eSignatures Act, and no plans have been proposed to encourage or mandate their uptake.

---


11.2.6 Statements from the service provider

Statements made by the service provider himself are integrated into the websites of the various single-points of contact as either web forms to be completed and signed or PDF files to be printed and sent via normal mail. It is not yet clear which requirements on electronic signatures will be imposed on such statements, beyond the comments made above. In many cases, for example the TYVI tax filing services and the statutory insurance notifications, the services are provided by various private enterprises.

The government has not seen it necessary to issue special requirements on electronic signing of different declarations, although this practice is encouraged by the authorities. In accordance with the Finnish legislation, the various eService providers use only user authentication to record the filings and do not require electronic signature certificates for this. In the case of the Katso authentication service (tax services) this is even more the case: in order to authenticate, the user can use an eID card only for registering to the service, after which the user will be given new Katso-credentials. The eServices accessible through the Katso authentication do not even support the eID card or the certificates stored on the card.

11.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

11.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As was noted above in the explanation of the TYVI and insurance services, the identification of the competent public administrations and private organisations and the interaction with them is already a core function of the services. This will thus remain the same after the implementation of the Services Directive: the eService providers and the BIS, which are acting as a PSC (through the EnterpriseFinland.fi portal), will still be used for informing about the service provider about the appropriate bodies that need to be communicated with. It remains to be seen whether the national portal service will also become responsible for interacting directly with these bodies.

With regard to the actual communication between the services and these administrations and/or organisations, it is currently being examined how these can be simplified and modernised, to ensure that the service provider will no longer have to correspond with any other entity than the single-point of contact. Service providers would probably provide all the needed documentation through the EnterpriseFinland.fi portal, but it is not yet clear how the relevant single-points of contact will then process this information in accordance with the procedures that have been defined for each specific service type. This scenario is not yet in place.
With regard to interactions with public administrations (such as the registration of enterprises in official databases, VAT registration, registration as an employer, etc.), the existing TYVI and statutory insurance reporting services are using web services. For communications with private organisations, most interactions will not be automated, and the services will also remained staffed in order to help and contact the competent organisations directly via any appropriate means – which may include e-mail, but also more traditional means such as fax, telephone, traditional mail or physical visits – to ensure that the information is processed correctly. BIS services have traditionally been offered only at offices thus a physical office service still exists, but TYVI tax services are purely online service and they can only be delivered physically in a tax office, if the online channel is not being used.

If service providers of other Member States rely on foreign electronic documentation which is difficult or impossible for the services to validate themselves, it is currently foreseen that this information will be validated through the IMI system. Obviously, this is regarded as a fallback solution which will only be used when needed, and not as a standard practice.

11.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Currently, the different eServices are available for all service providers in Finnish, Swedish and partly (though rarely) in English. As noted above, the web services are mostly run by private service providers and offered limited possibilities for direct interaction with the authorities at large. Since there is no cross-administration information exchange or case handling, the existing services cannot be considered to be PSCs.

Elements such as response time requirements, use of specific languages, and liability have not yet been reviewed, although it should be noted that the Act on Electronic Services and Communication in the Public Sector (13/2003) contains provisions on the rights, duties and responsibilities of the authorities and their customers in the context of electronic services and communication. The Act provides that service users may use digital signatures but, if the authenticity of an electronic document is not put in question, the authorities will have to accept also unsigned documents. With regards to service level and liability, the sender of the message is responsible for assuring that the submitted document is received by the authorities and that the document is verifiably authentic. The Act does not hold the authorities liable for anything else than having to accept electronic documents (non-discrimination of media) and ensuring that the services using electronic channels remain accessible and usable. The Act does not force the authorities to set up services using electronic documents.

With regard to communication with the service provider, no specific decisions have been made at this point yet. However, it seems likely that at an initial stage simple e-mail communication or a similarly accessible technology will be chosen. More complicated and/or highly secured solutions can be considered in the longer term.

181 The Internal Market Information System; see http://ec.europa.eu/idabc/en/document/5378/5970
183 Chapters 2 and 3 of the Act
When specific electronic documents (such as authorisations or licenses) must be delivered to the service provider, a number of possible solutions are still being considered, and it is not yet clear how this situation would be handled.

11.4 Assessment – Plans, progress and proposals for further harmonisation

11.4.1 Current plans and progress in the implementation of the Services Directive

As shown in the overview above, Finland already has a limited infrastructure in place that can be leveraged for the implementation of the Services Directive, in the form of the EnterpriseFinland.fi portal that already support part of the functions expected of the PSC; and in the form of the Business Information System (and related services) which acts as an official register of essential information related to service providers, including specific authorisations and fields of economic activity. The Finnish government plans to leverage this infrastructure in significant degree to in implementing the Directive, but combined with other ongoing eGovernment initiatives.

Specifically with regard to electronic documents, Finnish experience has been limited. This is to a large extent due to the role and use of authentic sources of information as a replacement of paper documents. As noted above, a fundamental principle behind Finnish eGovernment initiatives is that progress can best be made by completely changing paper based administrative processes and to building integrated information systems to link different authoritative data repositories from different administrations. These resources are then made available as free basic information services, or given access to for private or public information service organisations that provide specialised subscription and fee based service for companies and persons. In this regard, a growing number of authoritative electronic resources are made partly accessible to the general public and entirely accessible for specific trusted and mandated business service organisations. In general, an increasingly growing use of authoritative electronic resources in real time, makes the idea of formalised electronic documents a step backwards, as it would constitute a re-shaping of earlier formalities (i.e. turning paper documents into electronic ones), rather than eliminating them.

Thus, while the tasks of the EnterpriseFinand.fi portal and the technical infrastructure to support single-points of contact services will need to be updated as a part of the implementation of the Services Directive, the uptake of electronic documents is not expected to be a key part of this process. Rather, the existing portal and eServices will be extended to include additional information related to the service providers, including the specific authorisations that they have obtained from public or private sector bodies.

This does not necessarily mean that electronic documents would be entirely unused by the Finnish single-points of contact, but rather that they would not become a key part of the Finnish strategy to implement the Services Directive. If this would turn out to be necessary, it would be feasible to create electronic documents containing the registered information using any number of common standards. As already noted above, Finnish administrations have relied on Microsoft, Adobe and Web form products in the past to produce electronically signed documents, and this would be a possibility for the implementation of the Services Directive as well, if there would be a need to do this. However, generally speaking, the Finnish approach much favours the elimination of documents (paper based and electronically) and relying on the creation of trusted networks of authentic information instead, which can be accessed by different parties through specific web services.
11.4.2 Suggestions for further European support initiatives

Given the Finnish emphasis on authentic sources and web services rather than electronic documents, the creation and expansion of trusted networks to exchange authentic information between different parties would seem to be a favoured option. As an additional element, Finland would welcome further steps towards establishment of multilingual support for existing electronic documents and services in Europe. From a technical perspective, the Finnish infrastructure would be able to accommodate most widespread standards, so that there is no specific preference in this regard. Also issues related to “gap filler” services to accommodate various EU MS services with Finnish services are sought for, in order enable Finnish administrations to deliver electronic documents and web services for European service providers.

With regard to electronic signatures, it is not yet clear which signature solutions will be supported in cases where signatures will be required. In principle, the Finnish approach is envisaged to support the Finnish eID card and a limited number of certification service providers of other Member States, likely through a trusted list, but no official position has been taken on this.

It is not yet clear how this approach can be reconciled with the larger number of European CSPs in existence. A possible solution includes the integration of validation services that would allow a larger number of signatures to be validated, like in the case of the Large Scale Pilot Project PEPPOL\(^\text{184}\), where Finland is participating. In relation to signatures placed on electronic documents of other Member States, there is an interest in pursuing the option that was tested in Austria\(^\text{185}\), in which electronically signed documents are also provided with visual information regarding the essential characteristics of the signature and signatory (including specifically his/her legal capacity), along with contact information of the issuing authority. It would appear that this would be a relatively simple step if further harmonisation efforts are undertaken, which would greatly facilitate validation processes. Nevertheless the language issue is deemed primordial since validation of a signature (i.e. authorisation) requires also semantic understanding, which remains largely unresolved in the European context.

At any rate, key difficulties in practice include the determination of the reliability and responsibilities of service providers of other Member States, and the ownership of these CSPs, as it may be politically sensitive to support CSPs which are not under public sector supervision. Thus, the issue of electronic signature support is certainly a field where European initiatives could be useful in order to improve trust or facilitate validation of e-signatures. Another domain deemed important for the Finnish authorities, are initiatives to support better semantics for digital signature validation and authorisation.

\(^{184}\) Pan European Public Procurement Online, see: [http://www.peppol.eu/](http://www.peppol.eu/)

\(^{185}\) See e.g. [http://www.a-sit.at/pdfs/20060504%20eID%20Demonstrations.pdf](http://www.a-sit.at/pdfs/20060504%20eID%20Demonstrations.pdf), slide 11
12 France

12.1 General framework for electronic documents in eGovernment applications

12.1.1 Electronic documents in eGovernment applications

The ordinance n°2005-1516 of 8 December 2005\textsuperscript{186} has provided a legal framework for the development of e-administration. This Ordinance foresees the simplification of administrative e-procedures for users, defines the conditions for e-signatures of administrative acts, for the security and interoperability of electronic exchanges between users and administrative authorities and between these bodies, and finally provides for the creation of an online storage space for users. The reference to administrative authorities should be understood broadly as including not only the central government but also local authorities (collectivités territoriales) and public administrative institutions (établissements publics administratifs), bodies managing social protection regimes and public administrative institutions (établissements publics administratifs).

With regard to the signature of administrative acts, the Ordinance does not however refer to the general framework applicable to the private sector installed by Decree n°2001-272 of 30 March 2001, but to a procedure that should allow for the identification of the author of the signature, for linking the author to the signature and ensuring the integrity of the act, in conformity with the specifications contained in the General Security Directory (Référentiel Général de Sécurité)\textsuperscript{187}, specific to the public sector. The administrative authorities have to define the security level they want to apply for signature depending on the types of administrative acts they have to sign.

This General Security Directory defines the rules that information system functionalities should comply with. It defines security functions requirements such as electronic signature, authentication, confidentiality and time stamping. It distinguishes three security levels according to the sensitivity of the data exchanged and the risk of identity theft: middle, strong/standard and strengthened. The framework applies to security products and trustworthy service providers within electronic exchanges between users and public agencies and between public agencies. A signature certificate with a security level 3 is a qualified certificate with some interoperability features.

The French government defines a qualification program and delegates it to certifications bodies. These certifications bodies are accredited by a general accreditation body (the COFRAC Comité français d’accreditation) and qualify trust service providers, according to the requirements stated in the General Security Directory.


\textsuperscript{187} The decree relative to the General Security Directory and the General Security Directory were sent to the European Commission (directive 98/34/CE).
Despite this framework, electronic documents are not usually issued in the context of electronic procedures.

12.1.2 Electronic documents for the purposes of the implementation of the Services Directive

Article 8-V of the Act of 4 August 2008 about the modernization of economy has introduced a new provision to the Act n°94-126 of 11 of February 1994 about economic initiative and individual entrepreneurship that stipulates that services providers falling under the scope of application of the Service Directive can perform all required formalities and procedures for access to and exercise of its activity before the Centres of Formalities for Companies (Centres de formalités des entreprises, ‘CFE’), according to the conditions established in a decree adopted by the State Council. This decree is still pending of adoption. These centres are thus designated as Points of Single Contact for the purposes of article 8 of the Service Directive. In that sense, the Code of Commerce already acknowledges the possibility to perform the formalities relative to the creation and status modifications of companies via electronic means and defines its conditions (articles R123-20 to R123-27).

The CFEs have been shaped as Single Points of Contacts by the Act n°94-126 of 11 of February 1994 and are now regulated under the provisions of a dedicated section of the Regulatory Part of the Code of Commerce (Preliminary Section, Chapter III, Title II). They are thus fully operational. Seven networks exist, with different fields of competences relating to the activity and legal form of the company: Chamber of Commerce and Industry, Chamber of Craft Industry, Clerk of the Commercial Court, Chamber of Agriculture, Chamber of traditional inland watershipping, Social Security Contribution Collection Office, Tax Office.188

The CFEs should provide for submissions of one single file with all documents required for the creation of companies, the modifications of their status and the cessation of their activities. The CFEs proceed to a formal control of the documentation and transfer this documentation to competent authorities. It eases the procedures and formalities to be performed relative to the establishment of foreign professionals by the centralisation of the documentation to be sent to the relevant competent authorities. All legal, administrative, fiscal or statistical procedures foreseen by the legislation could be performed online, provided that the competent CFE offers this service.

Articles R123-21 to R123-27 defines the conditions for the submission of the unique file via electronic means. This service could be provided by CFEs or Court Clerks provided that they have the required technical equipment. There is thus, currently, no legal obligation for such entities to provide the service via electronic means. However, four of the existing CFEs networks (Chamber of Commerce and Industry, Clerks of Commercial Courts, Social Security Contribution Collection Office, Tax Office) provide for electronic submissions of documents.

188 For geographical and ratione materiae field of competence of each of these networks, see (in French) : http://annuaire-cfe.insee.fr/AnnuaireCFE/html/MissionCFE.htm
provide for electronic services with full coverage of their activities. The network of the Chamber of Craft Industry is currently implementing it, whereas the remaining two are still examining the issue. These last two networks however fall outside the scope of application of the Service Directive. In any case, the government is planning to launch a single website from which service providers will be able to submit their files to the competent CFE.

The service should be accessible online, secure and free, and should allow the declarant either to transmit the complete ‘unique file’, or to prepare this file in an interactive way and transmit it online. Moreover, when the declaration requires the registration of the Company to the Register of Commerce, the system should allow:

- the declarant to pay the requested fees online.
- the competent Court Clerks to receive the relevant documents to proceed to the registration. They should return receipt via electronic means to the declarant.
- the CFE to receive by electronic means the ‘unique file’.

Article R123-23 defines the content of the ‘unique file’. It should include the following documents (the electronic requirements for these documents should be determined by a ministerial decree still pending):

- The electronic version of the declaration form.
- The required documents in their electronic version, included where required, the mandate given to a representative, the constitutive acts having to be deposited. This excludes cases where paper-based originals are required.
- Certificates of having paid the requested fees.

When the documents submitted need to be signed, the declarant should use a secure e-signature as defined by Decree n°2001-272 of 30 March 2001. However, ‘simple’ electronic signatures can be used for the transfer of files requesting the creation of a company or the listing to the Register of Commerce.

The CFE should return a receipt via electronic means confirming the reception of the file to the declarant or his representative. This receipt should be attached if the declarant opts for submitting paper-based documents (e.g. authentic acts or original private acts).

Once the dossier is reputed complete and thus could be forwarded by the CFE to the competent authorities, the CFE will sign the receipt with a secure electronic signature and send it to the declarant via electronic means indicating the public authorities to which it is forwarded (art. R123-10) and other requested legal mentions (art. R123-16). The declarant can however request its transmission by traditional mail. A ministerial decree should determine the modalities of delivery of the electronic receipt.

If the declarant uses a service of temporary storage proposed by the CFE or the Court Clerk, the stored data should be deleted in a maximum period of one month. The declarant is warned by electronic means or by traditional mail before the deletion.
12.2 Specific document types

First of all, it is worth noting that copies are largely admitted by French public authorities. The submission of false copies is labelled as forgery and as such is criminally punished (article 441-1 Penal Code). The relation between users and public administration is thus largely facilitated and this reduces the need for electronic authentic documents to be issued by private organisations.

12.2.1 Extracts from commercial registers

All key information related to economically active independent entities in France is legally controlled by the Clerk of the Commercial Court (Greffier du tribunal de commerce) before its listing to the Register of Commerce. Extracts of such Register, the so called “extraits K-bis”, are given evidential value because they are checked by a public officer. Basic information stored about the registered entities includes:

- Informations relative to the company such as name, address, date of end of accounting year, capital, legal form, creation date, register number, object, etc.
- Informations relative to the civil status and contact details of legal representatives, share holders, members of board, statutory auditor

The information is updated in real time. It follows that the K-bis extract is only valid for a limited amount of time (three months). This information is available online from the database of the Clerk (the so called Infogreffe), but this has no evidential value. It is also possible to buy an extract online but it will be delivered on paper and by registered mail. The possibility to issue an electronic version of the ‘extrait K-bis’ with evidential value should however be contemplated and its modalities defined in a specific legal text.

12.2.2 Criminal records

Extracts from the penal register (also knows as « extrait de casier judiciaire, bulletin n°3″) exists in France but only in a paper format. Article R. 82 of the Penal procedure Code provides for the possibility to formulate the request via telematics means. The request can now be formulated online via the website www.service.pulic.fr where a specific form should be fulfilled by the user. The sollicitant of an extract from the penal register online has only to provide its identity (name, first name, date and place of birth) and declare on oath that the information provided is correct. Penal sanctions are foreseen for identity theft (article 433-23 of the Penal Code). The information provided by the user is

189 Identity theft will qualify as an offence in circumstances that lead or could have led to the initiation of a criminal prosecution against such a person (Article 434-23 of the Penal Code). Two elements should be present to qualify as a conduct of identity theft:
then checked by the Direction of criminal affairs except in cases where the applicant is born in a foreign country, his place of birth is unknown or if he is younger than 12 years-old. In these cases, the request should be accompanied by a civil status certificate (*justificatif d'état civil*). The Ministry of Justice has recently announced, during the ceremony surrounding the issue of the first electronic authentic act in France, that citizens will be able to require an electronic version of extracts from the penal register.\(^{190}\)

Moreover, in order to lighten the formalities for the creation of companies that requires to be listed in the Register of Commerce, and when character evidence (*condition de moralité*) should be provided, the declarant should only submit a bonafide statement (*déclaration sur l'honneur*). The Clerck of the Commercial Court will then check the penal register to authenticate the declaration.

### 12.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations, orders or stakeholder bodies. While it is difficult to obtain a complete overview, it does not appear that the extracts issued by such private organisations are commonly issued in a paper form. The legal possibility to do so exists, due to the implementation of the Signature Directive, but in practice only paper documents are issued.

Currently, no plans exist to make the use of electronic documents mandatory or to encourage them further.

### 12.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form. While it would be legally possible to do so under the terms of the eSignatures Act, in practice there seems to be no demand for electronic certificates, and so far there are no applications or services that require them, either in the public or private sector.

---

- the thief has to “assume the name of another person”. As of today, no judgement has been rendered in the sense that the concept of “name” could be understood to include IP addresses, email addresses or pseudonyms.\(^{189}\)
- “in circumstances that lead or could have led to the initiation of a criminal prosecution against such a person”.

In many cases, the sole act of assuming the name of another person will qualify as an offence. As a way of example, offences such as fraudulent representation\(^{189}\) (article 313-1 Penal Code), forgery (article 441-1 Penal Code) or public defamation (Article 29 of the Press Act of 29 July 1881) could be mentioned.

12.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications: generally, these could be private sectors issued documents for which only paper originals are available.

12.2.6 Statements from the service provider

Decree n°99-68 of 2 February 1999 about uploading administrative forms, as modified by a decree of 25 May 2001 about the simplification of administrative procedures, introduces the admissibility of electronic administrative forms. Since it entered into force, each new administrative form is given an electronic equivalent.

Article 3 and 5 of Ordinance n°2005-1516 stipulate that an electronic request requires the administration to return receipt of any request, declaration of presentation of document or payment by the solicitant within an e-service.

As mentioned above, most of CFEs and Court Clerks already offer a series of service of online submission of documents for the creation and status' modification of companies within the conditions set up by articles R123-20 to R123-27 of the Code of Commerce.
12.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

12.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

The functions of the CFEs, the modalities of transfer of ‘single files’ and liabilities are defined by the Code of Commerce (Preliminary Section of Chapter III, Title II of the Regulatory Part dedicated to CFEs) and thus by the State. The experience of CFEs is however taken into account for the definition of these functions.

Currently, CFEs transfer documents to competent authorities through EDI, broadly used by fiscal and social public authorities for massive exchanges of data. However, the technical features of the communication channels between CFEs and competent authorities relative to the Service Directive are still to be defined according to the results of the evaluation of the authorization regimes’ survey. The main nature of the French administrative division of powers implies that a significant number of decisions are taken at county level by prefectures. A technical dispositive that could be used by prefectures is thus currently being considered and its implementation studied.

12.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

CFEs currently transfer documents to company founders via Internet. However, in the light of the new requirements introduced by the Service Directive, work is being conducted in order to define the most suitable communication means. Friendliness and accessibility of the service for national and European service providers are set as objectives.
12.4 Assessment – Plans, progress and proposals for further harmonisation

12.4.1 Current plans and progress in the implementation of the Services Directive

As shown in the overview above, France has started to define the infrastructure for the implementation of the Service Directive, allowing for service providers falling under the scope of this Directive to perform all required formalities for access and exercise of their activity through one Single contact point, the Centres of formalities for Companies. These Centres have gained considerable experience since their creation in 1994 as Single Points of Contacts and accelerating substantially the process of companies’ creation and status modification. However, whereas the possibility to perform these formalities online is foreseen by the legislation, it is not yet fully implemented in practice as CFEs needs to be equipped with appropriate technologies. The problems of both limited competencies of CFEs (that cannot provide for all formalities as foreseen in the Service Directive in the current state of the legislation) and their unequal distribution among the territory are currently being dealt with by public authorities and networks of CFEs. The increased intervention of local authorities requires providing for specific solutions, as well as the communications channels to be re-asserted against the requirements of the Service Directive.

Specifically with regard to electronic documents, French experience has been mainly limited to ease procedures based on the use of electronic form available and the facilitation of communication channels through Internet. As copies are largely admitted by French public authorities, the need for users to provide electronic documents has been reduced to the minimum, replaced some times by bonafide statements where the authenticity of the data communicated are further checked by the competent public authority. On the other hand, electronic authentic documents, besides the legal and technical framework is ready, are not yet used in practice by public authorities. The Minister of Justice has indicated in that sense that a single website would be launched in 2009 for Justice where citizens will be able to request criminal records or copies of judgements. It is however difficult to determine whether this augurs a broader use of electronic documents by public authorities. Several Ministerial decrees are still pending in order to define e.g. the features of electronic receipt issued by CFEs to ensure the declarant that the file submitted is complete and being processed.

12.4.2 Suggestions for further European support initiatives

One of the main concerns of French public authorities is now related to the successful implementation of interoperable Single Point of Contacts by 2012. In that sense, France coordinates the preparation of the EU pilot project « SPOCS » and is thus expecting guidelines from the European Commission in that sense.

With regard to electronic signatures, French authorities are above all expecting feedback and support from the Commission for the implementation of ‘trusted lists’ relative to electronic signatures.

---

Concerns relate to avoiding that some Member States implement discriminating identification and authentication systems that would be excessive with regard to existing risks.
13 Germany

13.1 General framework for electronic documents in eGovernment applications

13.1.1 Electronic documents in eGovernment applications

13.1.1.1 Legal framework regarding the technical and procedural requirements

It is essential to understand that in Germany as a federal state legislative competences are split between Bund (Federation) and Länder (States). The general legislative competence lies with the Länder but the Grundgesetz (Constitution / basic law) nonetheless expressly assigns some competences to the Bund. As regards regulations addressing administrative procedures in particular, except for those concerning the federal administration, they are enacted by the Länder. So, apart from the Administrative Procedures Acts of the 16 Länder there is one Federal Bundesverwaltungsverfahrensgesetz (Administrative Procedures Act), to which the regulations of the different Länder Acts are related or even refer.

On all levels, Germany implemented regulations, that allow any kind of administrative process to be completed with electronic means (Elektronikanpassungsgesetz, Signaturgesetz, Erprobungsgesetze von Ländern, u.v.a.m.). This law is generally implemented in local, state and federal government. The EU services directive can fully rely on this infrastructure. According to a joint report of the state and the federal government, given with the co-operation of local government and the chambers, to the conference of the chancellor with the prime ministers of the german states, the implementation of the EU services directive will be based on this legal, organizational and technical infrastructure.

To further promote e-government and to implement the basic concepts of the services directive (i.a. “Member States shall ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant Point of Single Contact and with the relevant competent authorities”) in an extensive way within the administrative procedures (Verwaltungsverfahrensgesetz), Germany implemented a general point of single contact and new administrative procedures. So Germany relies on a continuation of the basic concepts of the services directive in further areas of the administration and it is fully prepared for such a development.

---

192 See Articles 30, 70 GG (GG: Grundgesetz - Basic Constitutional Law).

193 Art. 87 (1) GG.


195 E.g. LVwVfG BW: Administrative Procedures Act of Baden Württemberg.

196 E.g. Sec. 1 (1) NVwVfG (NVwVfG: Niedersächsisches Verwaltungsverfahrensgesetz - Administrative Procedures Act of Lower Saxony).
As an example for the new legislation, we provide:

Services Directive Article 3a (1) VwVfG which stipulates that the submission of electronic documents to administrative bodies is accepted as far as the recipient allows for such an submission process and offers the required means. According to sec. 3a (2) VwVfG documents which have to fulfil special formal requirements (e.g. if submission is required in writing) have to be signed with a “qualified electronic signature”. This electronic signature is only valid under the condition that the provisions stated in the SigG\textsuperscript{197} (which refers to the eSignatures Directive) are met.

Yet at regional level, based on their own legislative competence for the administrative procedures, the Länder and single municipalities have started to develop their individual eGovernment strategies. On the basis of regulations similar to the one in sec. 3a (federal) VwVfG\textsuperscript{198}, single municipalities or authorities now offer Internet platforms for their citizens to enable the handling of specific processes online\textsuperscript{199}. In most cases, these platforms are implemented in cooperation with a private service provider. However, they are not coordinated or consolidated centrally.

As far as the submission of electronic documents is concerned one can divide the Administrative Procedures Acts of the different Länder into three categories: The first one is characterized by its pure and broad reference to (mostly all of) the regulations of the federal act\textsuperscript{200}. Here, the legal situation regarding the possibility to communicate electronically and to obtain electronic documents is the same as on federal level, which has been described above. Secondly, some Länder have their own Act on administrative procedure but the regulations are identical to the ones in the VwVfG as far as the electronic communication is concerned\textsuperscript{201}. Thirdly, some Länder have their own and specific

\textsuperscript{197} SigG: Signaturgesetz – Law Governing Framework Conditions for Electronic Signatures. This law serves the implementation of the eSignature Directive, though the German concept of qualified electronic signature has no terminologic counterpiece in the Directive. It rather can be traced back to the type of signature described in Art. 2 no. 2 of the Directive, which has to fulfill two additional requirements: it has to be based on a valid qualified certificate (Annex I to the Directive) at the time of its creation and it further has to be generated by a secure signature-creation device (Annex III to the Directive).

\textsuperscript{198} Such a regulation concerning electronic communication either exists in a wording similar to the VwVfG (see e.g. sec. 1 (1) LVwVfG BW - Administrative Procedures Act of Baden-Württemberg) or is applicable by reference to the VwVfG (e.g. sec. 1 (1) VwVfG LSA – Administrative Procedures Act of Saxony-Anhalt). In Baden-Württemberg, for instance, the EAnpG: Elektronik-Anpassungsgesetz – Law Adapting Administrative Law to Modern Electronic Communication introduced sec. 3a LVwVfG adapting means of electronic communication to administrative law which did not only amend the LVwVfG, but amended several acts regarding the introduction of electronic communication or the expressive statement that electronic communication according to sec. 3a LVwVfG cannot be used to issue an administrative act.


\textsuperscript{200} Lower Saxony, Rhineland-Palatinate, Saxony, Saxony-Anhalt.

\textsuperscript{201} Bavaria, Berlin, Brandenburg, Bremen, Saarland, Thuringia.
regulations on electronic communication\textsuperscript{202}. In the \textit{Land} of Baden-Württemberg, for instance, electronic documents which are encrypted, signed, or with other special technical characteristics may be submitted only if the citizen and the authority have individually agreed so\textsuperscript{203}. Yet, in addition the authority may still demand the documents in written form\textsuperscript{204}. The VwVfG Hamburg and Schleswig-Holstein stipulates that the government of the \textit{Land} may decree that even electronic documents which do not contain a qualified electronic signature may replace the written form – if stipulated by a law of that \textit{Land}\textsuperscript{205}. In other Länder, again, communication via electronic means is only possible if the homepage of the authority says so\textsuperscript{206}.

For the future, although it is not considered as being necessary for the implementation of the Services Directive\textsuperscript{207}, the federal government intends to create a legal framework for a secure platform mainly for the exchange of E-Mails (so-called \textit{Bürgerportal or De-Mail}) as one tool to organize electronic communication. This platform shall set the standard for such platforms for the whole country. Although the Länder have the general legislative competence concerning administrative procedure, the federal government argues that the legislative competence for the \textit{Bund} results from art. 74 (1) no. 11, art. 72 (2) GG\textsuperscript{208} seeing that such a regulation would affect the economy countrywide and different regulations by the Länder would lead to disadvantages for the users. The testing of the platform shall start in 2009.\textsuperscript{209} A draft of the \textit{Bürgerportalgesetz}\textsuperscript{210} is under discussion and is part of the “E-Government-Program 2.0” of the federal government\textsuperscript{211}. It is meant to implement a platform, on which users may contract with private and public partners\textsuperscript{212} in a legally binding way. In addition, a mail service and an online post office box shall be offered. The platform and the services shall be put into effect by private service providers and shall be monitored by the Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security). The \textit{Bürgerportal} will be used both for services to which the Services Directive does and does not apply.\textsuperscript{213}

\begin{footnotes}
\item[203] Sec. 3a LVwVfG BW.
\item[204] Sec. 3a (4) LVwVfG BW, sec. 52a (4) LVwG SH (Schleswig-Holstein).
\item[205] Sec. 3a (4) HmbVwVfG (Hamburg), sec. 52a LVwG SH.
\item[206] Sec. 3a (1) HVwVfG (Hesse), sec. 3a (1) VwVfG NRW (North Rhine-Westphalia).
\item[207] See Reasons for the Law, p. 18/19; available in German at \url{https://www.e-konsultation.de/buergerportalgesetz/site/pictures/Referentenentwurf_Buergerportalgesetz.pdf} (last access Dec. 8, 2008).
\item[208] See Reasons, p. 18 (“Gesetzgebungskompetenz”, i.e. legislative competence).
\item[209] See \url{http://www.cio.bund.de/cln_093/DE/E-Government/E-Government-Programm/Buergerportale/buergerportale_node.html} (last access Dec. 8, 2008).
\item[210] Law of a Portal for Citizens.
\item[211] See \url{http://www.cio.bund.de/cln_102/DE/E-Government/E-Government-Programm/Buergerportale/buergerportale_node.html} (last access Dec. 8, 2008).
\item[212] Concerning the communication with public partners or authorities the law shall regulate the contact with federal authorities. See art. 3 of the draft concerning the Verwaltungszustellungsgesetz (Law on Service in Administrative Procedures).
\item[213] See the Federal report on Buergerportale (De-Mail) and EU-Services Directive; available in German at \url{http://www.cio.bund.de/cae/servlet/contentblob/77240/publicationFile/3968/langtext_buergerportale_download.pdf} (last access Dec. 5, 2008).
\end{footnotes}
It should be pointed out again, however, that the federal government does not consider the Services Directive applicable\(^{214}\). Nonetheless, the portal shall play a decisive role concerning the communication with the authorities and thus indirectly is an easy solution to allow for communication between citizens and authorities as required by art. 8 (1) of the Services Directive\(^{215}\).

Besides the Bürgerportal, which is yet to come, an electronic system for the exchange of documents between citizens, courts and authorities has already been installed, the so-called electronic court- and administrative post office box\(^{216}\) (EGVP\(^{217}\)). Using the “BundOnline-basic component data security”\(^{218}\) the EGVP basically is a virtual mail room. Up to now, however, just a few courts and administrations allow for the use of the EGVP\(^{219}\). The EGVP\(^{220}\) enables structured and unstructured Data Exchange based on OSCI communication protocol. In the project EINIG, in the North-Western region of the country, to implement the services directive, further actors such as the chamber of commerce, business development etc. have been included in the EGVP roll-out.

As for the Services Directive, it is important to point out that the exchange of electronic documents, e.g. e-mails or scanned documents, is considered sufficient to meet the requirements of the Services Directive. Nonetheless, many Länder and the federal government work on sophisticated and interoperable formats.

\(^{214}\) See reasons for the Law, p. 18/19; available in German at [https://www.e-konsultation.de/buergerportalgesetz/site/pictures/Referentenentwurf_Buergerportalgesetz.pdf](https://www.e-konsultation.de/buergerportalgesetz/site/pictures/Referentenentwurf_Buergerportalgesetz.pdf) (last access Dec. 8, 2008).


\(^{216}\) Designed by the Bundesverwaltungsgericht and the Bundesfinanzhof along with the Bundesamt für Sicherheit in der Informationstechnik and the Oberverwaltungsgericht Münster in consulting with the federal states Bremen and Hessen.

\(^{217}\) See [http://www.egvp.de](http://www.egvp.de), Elektronisches Gerichts- und Verwaltungspostfach.

\(^{218}\) [http://www.bund.de](http://www.bund.de); developed in lead of the Bundesministerium des Inneren, [http://www.bmi.bund.de](http://www.bmi.bund.de).


\(^{220}\) Information provided by the Land Bremen.
13.1.1.2 Technical Implementation

The EGVP\textsuperscript{221} is written in Java and requires the Java Runtime Environment\textsuperscript{222} (JRE). The application itself is based on the deployment- and activation mechanisms that are provided by Java Web Start\textsuperscript{223} which is included in the JRE.

Java Web Start is used to install the authentication application automatically including all required resources on the users’ PC. The resources provided by the server must be signed digitally. The webservice answers an HTTP-request on a JNLP\textsuperscript{224} resource file with the delivery of a “JNLP-File”\textsuperscript{225} to the user’s browser. This file specifies the required resources for the client application. The specified MIME-type\textsuperscript{226} causes the transfer of the resource definition to an executable for this MIME-Type\textsuperscript{227}. This executable now takes control over the download of the specific resources from the web-server and the activation of the Java application in a Java Virtual Machine (JVM).

Java Web Start then saves all resources addressed in a local cache. In case of a new activation of the link to the identical JNLP-File merely a differential download of the possibly altered parts of the application resources occurs. This mechanism assures the user to be always up-to-date and minimizes the download volume.

Furthermore, Java Web Start offers several security mechanisms. For example, on startup a user has to permit access to resources other than the “Java-Sandbox” on his PC explicitly\textsuperscript{228}. Also prior the installation of resources in the cache and the startup of the application the digital signature is verified and the certificates used are displayed to the user who may cancel the operation in case of doubt\textsuperscript{229}.

\begin{itemize}
\item \textsuperscript{221} This document relates to version 2.3.1 of the EGVP.
\item \textsuperscript{222} See: \url{http://java.sun.com}.
\item \textsuperscript{223} See: \url{http://java.sun.com/products/javawebstart/}.
\item \textsuperscript{224} Java Network Launching Protocol.
\item \textsuperscript{225} MIME-Type “application/x-java-jnlp-file jnlp.”
\item \textsuperscript{226} Multipurpose Internet Mail Extensions.
\item \textsuperscript{227} In this case javaws.exe, supplied by the Java JRE.
\item \textsuperscript{228} For example COM-Port for access the chip card reader, Printer etc.
\item \textsuperscript{229} See \url{http://www.egvp.de/pdf/technik/Betriebssysteme_EGVP.pdf}, version 1.9, 08.10.2008.
\end{itemize}
13.1.1.3 OSCI

OSCI\textsuperscript{230} is the eGovernment protocol standard. By using this protocol courts and authorities can communicate with their "costumers" (i.e. the parties to a proceeding or enrollees) over the Internet and can exchange legally binding, encrypted and digitally signed messages with each other. In this regard, contrasting previous communication protocols OSCI guarantees enhanced security by dividing user data and information data during transmission and by using a very secure encryption\textsuperscript{231}.

13.1.1.4 Communication of the EGVP over a network

The EGVP communicates over HTTP and SOAP over HTTP\textsuperscript{232}. In this process, the HTTP-Methods GET, HEAD and POST are used. The transport of OSCI-messages uses the HTTP-method POST. The TCP-ports depend on the server configuration in general 80/443 and 8080/8443. Authenticating proxies with the authentication schemes Basic and NTLM are supported. By using Java Web Start up to two password inputs are required due to the bos-application\textsuperscript{233} of Java Web Start which is not supplied by authentication information and has to query itself.

13.1.1.5 Transmission limitations

The standard transmission limitation in the EGVP for sending and receiving of messages averages 30 MB (and 100 Files). Files over 30 MB may exceptionally be submitted on CD-Rom.

13.1.1.6 Mailbox Size Limitations

The maximum number of messages averages 1000 messages per mailbox (Inbox, Queue and Sent) and a maximum size of 2 GB. These limitations are necessary to assure a fast performance of the EGVP.

\textsuperscript{230} Online Services Computer Interface, see http://www.osci.de.
\textsuperscript{231} Security review: http://www1.osci.de/sixcms/media.php/13/2002-07-29-OSCI-Bewertung-BSI.pdf
\textsuperscript{232} Simple Object Access Protocol; Hyper Text Transfer Protocol.
13.1.1.7 State of Use of the EGVP

In fact, until now just a few facilities of the German government make use of the EGVP. Additionally, some Länder have also installed individual solutions. For example, the Land Hamburg designed the “Hamburg Gateway” and (in contrast to the EGVP System) allows sending signed messages by standard mail via SMTP.

13.1.1.8 Specific requirements with regard to electronic signatures

Conventional service providers sign a variety of forms. In spite of the simplification of the authorization scheme under way and in spite of the members states efforts to use transactional systems, this requirement will sustain, e.g. for e-mail communication that runs necessarily in parallel to the use of transactional systems.

The qualified digital signature on an interoperable cross border level is required. Currently there are no functioning solutions available yet to address this issue.

The signature requirements are stipulated by the SigG. The creation of a qualified signature requires the use of a signature card issued by a trust centre. According to the SigG this is situated organizationally with the Bundesnetzagentur.

The Bundesnetzagentur provides a list of state of the art signature cards (signature creation device) and appropriate chipcard readers.

In order to use the EGVP two certificates are required:

- First of all, there is a certificate to encrypt the messages. The user can create a software-certificate (sw-certificate) for en- and decrypting messages. Additionally, this certificate (combined with the users’ password) is used to authenticate and log in to his mailbox in the EGVP.

- Secondly, a so-called qualified PKI-certificate on a signature card is required to sign qualified messages. This qualified signature is needed for some specific pleadings as mentioned in the SigG.

---

234 See https://gateway.hamburg.de, last access Dec. 4, 2008.
235 Simple Mail Transfer Protocol.
236 BNetzA – Bundesnetzagentur - Federal Network Agency for electricity, gas, telecommunications, postal and rail networks.
One should point out that the cross border interoperability of qualified signatures, preferably in combination with a unique interface for the common use of all European qualified signatures, is essential by mid 2009 to allow testing.238

13.1.1.9 Technical requirements regulated through ‘soft law’

Germany made an enormous effort and provided a general action plan for local, state and federal government as well as chambers for the national implementation of the EU Services Directive within Deutschland-Online (so called Projektbericht des Deutschland-Online Vorhabens “Nationale IT-Umsetzung der EU Dienstleistungsrichtlinie”). This paper was worked out with the help of the German IT industry and E-Government research. It describes hundreds of suitable technical, organizational and legal solutions and gives an overview of the standards, guidelines, policies etc.

Document types for use within the EGVP, for example, must be explicitly permitted through decree-law by the respective court or authority. In general, the following document types are accepted:

<table>
<thead>
<tr>
<th>Type</th>
<th>Limitations</th>
</tr>
</thead>
</table>
| ASCII (American Standard Code for Information Interchange) | - without version limitation  
- as pure text without formatting or special characters                  |
| Unicode                                   | - without version limitation                                                |
| Microsoft RTF (Rich Text Format)          | - version 1.0 through 1.6 without Extension for Word 2000                   |
| Adobe PDF (Portable Document Format)      | - version 1.0 through 1.4 (if readable with Adobe Reader 6.0)              |
| XML (Extensible Markup Language)          | - if displayable with Internet Explorer 5.x                                |
| Microsoft Word                           | - no active components  
- Word 97, Word 2000 (Version 8 or 9), Word XP                            |
| Open Office text documents                | - no active components  
- version 1.1                                                                |
| TIFF (Tagged Image File Format)           | - version 6 or lower                                                       |

Files can be compressed by ZIP239. In this case, the signature must refer to the original document file rather than the compressed file.

Further standards for electronic communication are SAGA standards and best practice standards used within IDAbc / ISA etc as well.240

238 Information provided by the Land Baden-Württemberg.
240 Information provided by the Land Baden-Württemberg.
13.1.2 Electronic documents for the purposes of the implementation of the Services Directive

13.1.2.1 Acceptance of electronic documents or plans, respectively

Electronic documents are accepted as an evident document if provided with an eSignature. If requested by the applicant the administrative procedure shall be rolled out electronically (based on Art. 8 Services Directive) regardless of the requirement to use electronic documents. If the procedure is conducted electronically but in absence of electronic documents, the requirements set by Art. 8 are met.

Each German Land has set its own conditions regarding receipt and acceptance of electronic documents. Where required, an eSignature must be used. The corresponding middleware is interoperable with eSignatures from Bulgaria, Finland and Switzerland. Solutions for Member State-wide interoperability are currently developed in the ICT-PSP Pilot A - PEPPOL project. The second Land whose authorities communicate via EGVP is Lower Saxony. In the Land Baden-Württemberg, only the courts but not the authorities make use of the EGVP.

Governikus and VPS-Software form the essential components of the technical infrastructure of the EGVP, and are being used, for instance, by the Land Baden-Württemberg.

13.1.2.2 Legal requirements

So far there are no legal requirements that could ensure standardized document formats or data types in Germany, at least not in a comprehensive way covering all fields. As far as can be seen, the Services Directive does not contain any specific provisions on that issue, but stipulates that standards regarding the data type have to be met in order to ensure interoperability with external, inter-organizational services.

---

241 However, not all authorities use EGVP, but only a few Landkreise and Gemeinden, see http://www.egvp.de/behoerden/index.php (last access Dec. 17, 2008).
243 See http://213.216.17.150/DOL/Anlagen/Anlage_A14_Anwendungen_auf_Basis_OSCI.pdf (last access Dec. 17, 2008).
244 Information provided by the Land Baden-Württemberg.
245 Information provided by Federal Ministry of the Interior, IT Division.
13.1.3 Services Directive

13.1.3.1 Technical requirements (document types and formats, signature standards, communication protocols)

As far as IT issues are concerned, the (internal German) project report on the implementation of the Services Directive recommends to use the syntax XML as basis for the display of the semantics within specific administrative procedures (*Fachverfahren*).\(^{246}\)

In the *Land* Baden-Württemberg, for instance, the EA (PSC) is currently being implemented. Both for procedures under the Services Directive and other eGovernment procedures it has become the standard to accept and process electronic documents. A service provider may fill in all the necessary forms online (e.g. those required for setting up a business) at the One-Stop-Government portal www.service-vw.de), and may upload the required documents, hence in an electronic format (e.g. the *Meisterbrief* (master craftsman’s diploma) as pdf). The service provider may obtain information on the status of his application online and further inquiries may be sent by e-mail. Electronic interfaces enable other authorities and organizations to participate in the process electronically.

The different technologies available are:\(^{248}\)

1. In Baden-Württemberg, the technology for implementing process oriented PSC on the basis of personalized safe document storage is available at the administrational portal www.service-bw.de.
2. Virtual message boxes are available, too, working with digital signatures of all classes (e.g. Governikus, OSCI, service-bw, VPS of DZ BW).

To take another example, Bremen started an interregional ICT-measure in January 2008 to develop solutions for the technical implementation of the PSC. The joint venture named EINIG (www.vir-nordwest.de/einig) is conducted with local municipalities in Lower Saxony, ICT-Companies and communal interest groups. The architecture is mainly based on OSCI Standard and web services technology using existing solutions e.g. the German Administration Registry DVDV, S.A.F.E. etc.. The project is funded by the Metropolitan Region of Oldenburg-Bremen Northwest e.V.

13.1.3.2 Status of plans

The German *Länder*\(^{250}\) have started legislative measures to install PSC but implementation differs from the regional level to local authorities. Bremen, Lower Saxony and North Rhine-Westphalia, for

\(^{246}\) Information provided by Federal Ministry of the Interior, IT Division.

\(^{247}\) Information provided by the *Land* Baden-Württemberg.

\(^{248}\) Information provided by the *Land* Baden-Württemberg.

\(^{249}\) Information provided by the *Land* Bremen.

\(^{250}\) Information provided by the *Land* Bremen.
example, will implement PSC on the level of local authorities. To date Bremen is trialing a fully
electronic information and application service prototype.
13.2 Specific document types

13.2.1 Extracts from commercial registers

Sec. 8 (1) HGB\(^{251}\) stipulates that the commercial registers are to be held by the courts in an electronic format. Anyone can inspect the register for informational reasons. Therefore, the Länder's administrations of justice had to define an electronic system of information and communication, which allows the citizens to gain access to the register (sec. 9 (1) 2\(^{nd}\) sentence HGB). The Länder established the Common Commercial Register Portal\(^{252}\) in accordance to sec. 9 (1) 4\(^{th}\) sentence HGB. This platform allows saving or printing register extracts on demand. Regularly, this service is free of charge.

More specifically, three types of extracts are offered: extracts from the current register (including all valid entries), chronological extracts (including all data since the swap to the electronic form), and historical extracts (including all data since the swap to the electronic form)\(^{253}\).

Among other things, the printouts contain information on the company, type of legal entity, subject of its business activity, registered office, individuals with representative powers and, if applicable, registered capital of the company\(^{254}\). These documents are not bound to a certain file-format.

The electronic extract is of the same legal value as the former paper based extract.\(^{255}\) Thus, although citizens can still order paper based extracts (sec. 9 (4) HGB), they are not necessary anymore. The authenticity of the extracts, i.e. the concordance of the extract with the complete electronic commercial register, can only be proven by a separate request of accreditation to the court in charge (sec. 9 (3) HGB), using a qualified electronic signature according to sec.(2)9, 3 SigG. However, this accreditation does not prove the correctness of the entries of the register.\(^{256}\)

\(^{251}\) HGB – *Handelsgesetzbuch* - Code of Commerce.

\(^{252}\) See http://www.handelsregister.de/ (last access Dec. 8, 2008).

\(^{253}\) See http://www.justiz.de/Onlinedienste/Registerauskunft/index.php (last access Dec. 8, 2008).

\(^{254}\) See https://www.handelsregister.de/rp_web/div/info-lang/en-GB.pdf (last access Dec. 8, 2008).

\(^{255}\) See Baumbach/Hopt, Commentary on HGB, 33\(^{rd}\) ed. (2008), sec. 9, recital 3.

\(^{256}\) See Baumbach/Hopt, Commentary on HGB, 33\(^{rd}\) ed. (2008), sec. 9, recital 7.
There are similar rulings on the company register\textsuperscript{257}, which is an official platform that allows access to a collection of information from several registers on business entities, e.g. the commercial register, the registers on cooperatives and partnerships as well as announcements according to the law of shares (sec. 8b, sec. 9 (6) HGB).

If the extracts from the registers are accompanied and accredited by an electronic signature, the validity of the electronic signature can be determined by means of the OSCI-Standard.\textsuperscript{258} The OSCI standard has set relevant requirements.\textsuperscript{259}

\textbf{13.2.2 Criminal Records}

In Germany extracts from the Federal Central Criminal Register(also known as certificate of good conduct\textsuperscript{260}) are issued to nationals personally or – if the criminal record is ordered to be submitted to an authority – directly to the authority as requested by the citizen. The application for the issue of a criminal record has to be filed in person or by a representative providing a certified signature at the local municipality that passes the application on to the federal register authority\textsuperscript{261} which is part of the Federal Ministry of Justice\textsuperscript{262}.

The generic legal frame is the BZRG\textsuperscript{263}. Its administrative regulation does not provide for rules for an electronic document. Only the communication between public administrations and the federal register authority concerning criminal records is partly arranged on an electronic basis (sec. 21a BZRG). If the criminal record is issued to the citizen directly, it is solely issued on paper and sent by traditional mail (sec. 30 (1) BZRG).

In a cabinet decision of Oct. 15, 2008\textsuperscript{264}, the German Federal Government decided to revise the administrative regulation concerning the execution of the federal central criminal register act\textsuperscript{265},

\textsuperscript{257} Unternehmensregister, see https://www.unternehmensregister.de/ (last access Dec. 9, 2008).
\textsuperscript{258} Information provided by the Land Bremen.
\textsuperscript{259} See www.osci.de; Information provided by the Land Bremen.
\textsuperscript{260} Führungszeugnis.
\textsuperscript{261} Bundeszentralregister.
\textsuperscript{262} See http://www.bundesjustizamt.de/nn_257894/DE/Das_20BFJ/DasBFJ__node.html?__nqn=true (last access Dec. 9, 2008).
\textsuperscript{264} Bundesrat-Drucksache [BR-Drs.] (Official Record of the German Federal Council) no. 763/08 available at http://www.umwelt-online.de/PDFBR/2008/0763_2D08.pdf (last access Dec. 8, 2008).
designated to come into effect at the beginning of the year 2009. The federal register authority is designated to continue issuing the extracts on paper (sec. 11 (2) BZRGVwV). There are only two exceptions to this: The new Germany-wide system requires electronic transmission of extracts of criminal records between the federal criminal register and public authorities as well as courts (sec. 11 (3) BZRGVwV). The aim is to reduce time of transmission and to facilitate bureaucratic effort. Extracts of the criminal record directly issued to the citizen will still be provided on paper.

At the time of writing, electronic transmission of criminal records between the federal register and authorities requiring an extract from a register in order to fulfill their tasks (extracts according to sec. 31 BZRG) is within a test phase. Citizens may request an extract via electronic communication with the federal register but they further still get the extract printed on forgery-proof paper sent by traditional mail.

Another register that contains penalties, administrative fines and administrative decisions concerning the commercial activities is the Central Register of Companies which is based on the rules in sec. 149 GewO and is filed by the Federal office of Justice. In Germany, national natural or legal persons may request information on their entries in this register at the Trade Office in whose jurisdiction the applicant has their residence or head office. The procedure mainly corresponds to the one described above regarding criminal records. The information is provided on paper only. Presently there are no ambitions to issue these extracts to nationals in the format of an electronic document. Nevertheless, the claim for an extract which is only used for private purpose (sec. 150 (1) GewO) or which is to be submitted to another authority (sec. 150 (5) GewO) can already be submitted electronically directly to the Federal Office of Justice.

### 13.2.3 Extracts from professional registers

---

265 BZRGVwV: Allgemeine Verwaltungsvorschrift zur Durchführung des Bundeszentralregistergesetzes - administrative regulation concerning the execution of the federal central criminal register act.

266 See sec. 21 BZRGVwV.

267 See Reasons of the cabinet decision, BR-Drs. 763/08, p. 1, A.


270 Gewerbezentralregister.


Professional registers can be divided into two general categories according to the organization that collects and administers the relevant data: First, there is the official Business Register\(^{273}\) containing the information which have to be submitted by the entrepreneurs according to sec. 14 GewO. In general, it is managed at local government level (see sec. 155 GewO\(^{274}\) i.c.w. federal state law\(^ {275}\)) including all standing (non mobile) businesses\(^ {276}\) of the local district. Some professions do not have to register in the Business Register, especially the so-called Freelance Professions.\(^ {277}\) In contrast to the commercial register on the basis of the HGB, the Business Register is a non-public register. However, the government may issue basic extracts if requested by a person with legitimate interests (sec. 14 (8) 1\(^ {st}\) sentence GewO), or even the complete entry if the applicant meets the requirements of sec. 14 (8) 2\(^ {nd}\) sent. GewO. At present, there is a form of electronic Business Register but it is used for internal, administrative exchange only.\(^ {278}\)

In order to circumvent the formal requirements otherwise necessary for obtaining information on a company many local governments further provide their own mercantile directory in order to offer a central and free service. Companies have to enlist themselves. Some of these registers have been checked against the data provided by the Business Register.\(^ {279}\)

The second category of official registers covers registers and lists kept by professional associations, e.g. the Chambers of Crafts or the Chambers of Engineers. Those associations mostly offer access to their lists digitally.\(^ {280}\)

\(^{273}\) Gewerberegister.


\(^{275}\) An overview about the different federal state regulations is given by Tettinger in Tettinger/Wank, Gewerbeordnung – Kommentar, 7\(^ {th}\) Ed. Munich 2004, sec. 155, recital 7.

\(^{276}\) Stehendes Gewerbe.

\(^{277}\) Cf. sec. 6 sec. 1 GewO.

\(^{278}\) Cf. for example the press release by the “Kommunale Informationsverarbeitung Sachsen” concerning the introduction of the electronic business register in 2005, available at [http://www.kisa.it/kisa/content/1004/05072005122356.asp](http://www.kisa.it/kisa/content/1004/05072005122356.asp) (last access Dec. 8, 2008).

\(^{279}\) A platform that includes such an verification is provided in the Free State of Saxony available at [http://www.saechsisches-branchenverzeichnis.de](http://www.saechsisches-branchenverzeichnis.de) (last access Dec. 8, 2008).

\(^{280}\) Examples of such services are the services of the different cambers of craft, most of them are available at [http://www.handwerkskammer.de/?page_id=24](http://www.handwerkskammer.de/?page_id=24); the register of the Chamber of Engineers in North Rhine-Westphalia, available at [http://www.ikbaunrw.de/ind.php](http://www.ikbaunrw.de/ind.php); or the central registers of the German Federal Bar, available at [http://www.rechtsanwaltsregister.org/Impressum.aspx?lang=en](http://www.rechtsanwaltsregister.org/Impressum.aspx?lang=en) (all accessed Dec. 8 2008).
13.2.4 Certificates of insurance

Commonly, certificates of insurance are not issued in an electronic form. Although, it would be possible legally only some insurance companies provide digital certificates of insurance.\textsuperscript{282} And these certificates are provided without qualified electronic signature but with a statement along the lines of: “This document has been generated by a computer and is valid without a signature.” As a consequence, these documents do not fulfill the requirements of a qualified signature according to sec. 2 no. 3 SigG. Instead, they have the legal status of a document in textform (sec. 126b BGB\textsuperscript{283}), which is not to be confused with a document that fulfills the stronger criteria of written form according to sec. 126 BGB. As a consequence, these documents cannot be used for formal correspondence if written form is required.\textsuperscript{284} Nonetheless, it offers a quick service for cases where such requirements do not have to be met.

If the document has to be provided in written form it is common for the insured person to order such a certificate by e-mail or telephone and to receive them by traditional mail in written (paper) form.

13.2.5 Proofs of Qualification

In general, these documents, diploma as well as other proofs of qualification, are neither issued nor accepted in digital form. For employer's references the electronic form is expressly forbidden by sec. 109 (3)GewO providing an exception to sec. 126b BGB.\textsuperscript{285} The reason is to prevent a discrimination of small and medium sized businesses and to provide the employee with a certificate that is accepted by all companies independent from their technical equipment.\textsuperscript{286}

\footnotesize
\begin{itemize}
\item \textsuperscript{281} Versicherungsbescheinigung.
\item \textsuperscript{282} For example the compulsory health insurance fund “Barmer” provides this service, available at http://www.barcharr.de/barcharr/web/Portale/Versichertenportal/Formulare_20und_20Bescheinigungen/Bescheinigungen.html (accessed Dec. 9, 2008).
\item \textsuperscript{283} The German Civil code (BGB) is available at http://www.gesetze-im-internet.de/englisch_bgb/index.html (accessed Dec. 9, 2008).
\item \textsuperscript{284} Cf. Spindler/Weber in Spindler/Schuster, Recht der elektronischen Medien, 1. Ed(2008), sec.126b BGB m.n. 8f.
\item \textsuperscript{286} Cf. the explanatory memorandum according sec. 109 GewO; BT Drs 14/8796 p. 25f available at: http://dip21.bundestag.de/dip21/btd/14/087/1408796.pdf (accessed Dec. 8, 2008).
\end{itemize}
To provide additional security, the Mannheim University of Applied Sciences, for instance, uses a digital signature that allows a digital verification of their diploma.\textsuperscript{287}

Irrespective of this exception electronic copies are occasionally presented in the form of unsigned documents (scans), usually during the first steps of an application procedure.\textsuperscript{288} Within the further application process, the original documents or duly certified copies will be demanded in paper form.

13.2.5.1 Plans to encourage the issuing of documents typically issued by private organizations in electronic form

As mentioned before, Germany\textsuperscript{289} is developing De-Mail as a common electronic delivery system, which is to be established by different private service providers under the supervision of the German government. De-Mail can be used by citizens, corporations, public authorities and others without any limitations. The specification of the legal and technical framework is in progress and will be proved in a pilot project in the 3\textsuperscript{rd} and 4\textsuperscript{th} quarter of 2009.

The technical framework is based on the well-known Internet email. For De-Mail a different standard for email communication was profiled and expanded to fulfill all requirements for confidentiality, integrity, authenticity, traceability, availability, pseudonymity and acceptability on all business needs.

The legal framework is described in a new law Bürgerportalgesetz (available as draft) and a certification framework for the De-Mail provider.

All users of these services have to be registered with different types of identification attributes and must be identified. It is possible to record profession and qualifications like in a commercial register. These attributes can be used for the identification process as part of the De-Mail service De-Ident.

13.2.5.2 Requirements regarding acceptance of electronic documents typically issued by private organizations

Under sec. 5 (5) VwZG\textsuperscript{290}, the administration may currently deliver an electronic (signed) document to every recipient who established a reception portal for this type of document. This document has to be provided with an electronic signature according to the SigG. The amendment of the VwZG

\textsuperscript{287} The verification service is available at https://zeugnis.hs-mannheim.de/ (accessed Dec. 9, 2008).


\textsuperscript{289} Information provided by the Federal Ministry of the Interior, IT Division.

implementing the Services Directive intends to make delivery in electronic form obligatory if the recipient may – on the grounds of a respective provision–request that the administrative procedure is carried out electronically. Yet, be it that electronic delivery is optional or obligatory, it is necessary to accompany the document with a qualified electronic signature. Additionally, the public authority has to secure the document against any unauthorized access by any third party. Additional to the demands of an electronic signature the public authority has to secure the document against the unauthorized access by any third party.

13.2.6 Statements from the service provider

13.2.6.1 Obligation to use standardized electronic forms

During the registration process the subscriber has to deliver an original extract from a commercial request or other official documents with a confirmation of the validity of the attribute value. Otherwise the attribute value as part of the user registration dataset will be marked as “not approved”.

In Bremen, for instance, the service provider has to deliver his information by means of PSC via OSCI-Transport.

13.2.6.2 Process for delivering electronic statements

Due to the federal structure of Germany, the procedure of how service providers may deliver their statements differ. In some Länder, the PSC will ask for the necessary data by webform and will forward the received information to the authority by XML.

Furthermore, a service provider could also communicate via De-Mail. The De-Mail portal provides the possibility to identify the sender by using De-Ident.

De-Ident is an electronic De-Mail service for delivering an ident card which contains a defined subset of identification attributes. There are different types of De-Mail ident cards, i.e. age card, citizen identity card, corporation card. The following process could be used:

---

291 Information provided by BMI department V II 3.
292 Information provided by Federal Ministry of the Interior, IT Division.
293 Information provided by the Land Bremen.
294 See part 13.2.6.2, page 3.
295 Information provided by Federal Ministry of the Interior, IT Division 2.
296 Information provided by Federal Ministry of the Interior, IT Division 1.
1. The authorized De-Mail user requests to submit an ident card to a De-Mail recipient.
2. The De-Mail provider generates the ident card according to the user request, signs it with a qualified electronic signature and submits the ident card via De-Mail to the De-Mail recipient (i.e. a public authority).
3. The recipient receives the De-Mail which contains the ident card and can verify the signature and read the content of the ident card.

The ident card will be delivered in different formats: SAML Version 2 Token and in common readable PDF format. Afterwards the recipient can copy the identity attribute information in their own accounting or customer relation management system.

In Bremen\textsuperscript{297}, for instance, the service provider will communicate with the PSC via OSCI-Transport. It is likely that other governments will use the same technology as OSCI-Transport is part of the “blueprint” for the technical implementation of the EU Services Directive, which was jointly written by federal and state governments.

13.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

13.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organizations

As it comes to the question of whether any advanced/web-service oriented standard or communication protocol is being used, in Bremen\textsuperscript{298}, for instance, the OSCI-Transport is used widely in civil registration and court areas, both areas which are relevant to the EU Services Directive. For example, all notaries have to use OSCI-Transport based solutions when registering new companies. Therefore, solutions for EU Services Directive will build on these standards.

Also, Germany is involved in the CIP PSP Large Scale Pilot “SPOCS”, in which a specific work package will deal with the common specification of interchangeable middwares. The OSCI-Coordination office is involved in these endeavors and actively works with PRESTO and eLink projects together to agree on common solutions. Furthermore, the Large Scale Pilot “PEPPOL”, which is focusing on procurement, is working on a common technical infrastructure labeled “PEDRI”. This platform will be interoperable with OSCI-Transport, and can serve as a good solution for the technical implementation of cross-border scenarios.

The amendments to the Law on Service in Administrative Procedures, which stipulate the introduction of an obligatory electronic service including deemed delivery and substantiation if service is being disputed, are likely to come into effect before the end of 2008. In a second step, the \textit{Länder} will

\textsuperscript{297} Information provided by the \textit{Land} Bremen.

\textsuperscript{298} Information provided by the \textit{Land} Bremen.
amend their Laws on Service in Administrative Procedures according to the regulations within the federal Law on Service in Administrative Procedures.\footnote{299}

13.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

First, Bremen, for instance, does not need to change its legal framework for the delivery of documents by the administrations to the service provider.\footnote{300}

Regarding the question whether specific technical requirements have already been defined for the delivery process, the newly introduced sec. 5 (7) VwZG provides that the recipient is to send an acknowledgment of receipt to the delivering authority as a proof of receipt.\footnote{301} This acknowledgement can be sent by traditional or electronic mail. If the authority does not receive any acknowledgement of receipt until 3 days after delivery of the document, the document is deemed to be delivered. Delivery is not deemed to have occurred if the recipient can substantiate that he received the document at a later stage or not at all. Substantiation requires that the recipient presents conclusive facts for example by way of a screen shot, which detail that the document was not delivered or delivered later than the third day after sending. Apart from this, there are not further rules addressing the technical requirements within the VwZG.

However, the Länder may have specified further technical requirements.\footnote{302} Bremen accepts electronic documents by the free of charge software egvp.de, based on the communication protocol OSCI, combined with qualified electronic signatures.

Regarding the current status of the implementation of these plans, the German e-government project “Bürgerportale” which defines the legal, technical and certification framework for De-Mail was established at the end of 2006.\footnote{303} Different internet mail service providers, banks and saving banks, consulting agencies, insurance companies, public authorities and industrial corporations are part of the project team. The technical and certification framework currently is in its final adjustment process involving all participants. In the beginning of 2009, the technical framework will be established. In 3rd and 4th quarter of 2009 the technical implementation will be realized for a De-Mail pilot phase to verify the acceptance of the services by the potential users. After the law’s publication, the certification process of De-Mail service providers can be established and the service providers can request the different needed certificates for De-Mail functionality, IT security, Data privacy and for consumer protection. In 2010 the first De-Mail providers will go public with their certified and approved De-Mail services.

---

\footnote{299} Information provided by Federal Ministry of the Interior, Division VII 3.
\footnote{300} Information provided by the Land Bremen.
\footnote{301} Information provided by Federal Ministry of the Interior, Division V II 3.
\footnote{302} Information provided by the Land Bremen.
\footnote{303} Information provided by Federal Ministry of the Interior, IT Division 1.
Regardless of these initiatives, all competent authorities and PSC with regard to the services directive and 71a- 71e VwVfG will need to be able to at least receive and send electronic documents by December 28th, 2009.

13.4 Assessment – Plans, progress and proposals for further harmonisation

13.4.1 Other Points to Stress

The Land Baden-Württemberg informs that its One-Stop-Government-Portal (www.service-bw.de) is programmed like other modern web-based applications which can be handled easily and intuitively, while keeping a high security level and the prerequisites regarding the user’s technical equipment low.304 A service provider only needs a personal computer, a browser which is up to date (such as Internet Explorer or Firefox) and internet access. Documents to be uploaded can be formatted as pdf preferably, but may be submitted in other pixel true graphic formats (such as tiff, jpg, gif), too, if they paper based documents had to be scanned. The authority itself stores its notifications as pdf on the OSG-portal from where the service provider can download the notification. Alternatively, the authority submits the file as an attachment to an e-mail. Other data formats are not necessary. Inter-authority and intra-authority communication may use other formats like Word-doc.

It shall be pointed out again, that Germany is involved in the SPOCS project (see above).305

13.4.2 Possible European Initiatives

Following from the German XDLR-initiative, the Federal Ministry of the Interior306 suggests that – in the long run - a XML-Standard which is, to a certain extent at least, internationally interoperable shall be developed on EU-level. In the course of this project, which has not yet started though, a federal standardized XÖV307 for all the communication interfaces (e.g. for communication between EA and technical authorities, between EA and EA etc.) is to be developed. Identifying communication interfaces (in Germany, there are 6 at the moment) will certainly exist in other EU member states as well. Therefore, the idea is to focus on the development of an XML-Standard on the European level.

304 Information provided by Baden-Württemberg.
305 Information provided by Bremen.
306 Information provided by the Federal Ministry of the Interior, IT Division.
307 XÖV: XML-Standardisierung in der Öffentliche Verwaltung – abbreviation for xml standardisation within the public administration. For further information see http://www.standardisierung.deutschland-online.de.
14 Greece

14.1 General framework for electronic documents in eGovernment applications

14.1.1 Electronic documents in eGovernment applications

In Greece the presence of public administration bodies on the Internet is, with a few exceptions, limited to the provision of informative material for the services they offer. Many public administration bodies also offer on their website in electronic form application forms and other documents that need to be filled in for the carrying out of transactions between the citizens or enterprises and the specific body. In the few cases where documents are actually provided to the citizens in electronic form, they are usually scanned .pdf files. The major problem today with regard to the provision of eGovernment services (including the provision of electronic documents) is that competent authorities are reluctant to provide eGovernment services because they cannot support the ICT part of the service. In addition, most eGovernment applications currently face the problem (which subsequently affects the provision of electronic documents) of secure authentication of the citizens. Currently, as it will be further elaborated below, the public administration bodies require the authentication of their users via a username-password system. It is obvious that various dangers are inherent in this choice, as anybody who can obtain via any means the username and password of a citizen can further obtain their certificates and interact with the public administration bodies. However, even eGovernment services where authentication via username and password would be sufficient in terms of risk assessment, have still not been realised to a sufficient extent. This problem, along with many more, is being dealt with in a broad project on “The Greek eGovernment Service Provisioning Framework and Interoperability Standards”

308, the main purpose of which is to define acceptable steps and specifications for the provision of eGovernment services.

The “Greek eGovernment Service Provisioning Framework and Interoperability Standards” or shorter “Greek eGovernment Interoperability Framework” (Greek eGIF)309 defines standards, specifications and rules for the development and deployment of web-based front and back office systems (including the creation and exchange of electronic documents) for the Greek Public Administration, at national and local level, which will accelerate the development of electronic collaboration of public agencies, for the delivery of high quality and secure one-stop eGovernment services to businesses, citizens and other public bodies. The Greek Interoperability Framework is in conformance with the European Interoperability Framework (EIF) and applies best practices from relevant international standardisation Greek eGIF Building Blocks.

The Greek eGovernment Interoperability Framework consists of the following building blocks:


The Certification Framework for Public Administration Sites and Portals, which specifies the directions and standards to be followed by the public agencies at central or local level, when designing, developing and deploying eGovernment portals of the Public Administration and supporting e-government services.

The Interoperability and Electronic Services Provisioning Framework, which defines the basic principles and the general strategy to be followed by the public agencies, when developing e-government Information Systems. It also provides organisational and semantic interoperability guidelines, as well as the technical specifications and standards that should be used for the communication and the efficient exchange of information between e-government systems, aiming to the provision of integrated and interoperable e-government services.

The Digital Authentication Framework, which sets the standards, the procedures and the technologies required for the registration, identification and authentication of the eGovernment services users, including citizens, businesses, public authorities and civil servants. It also aims at creating an integrated and coherent set of policies regarding Digital Certificates and Public Key Infrastructures.

The Documentation Model for Public Administration Processes and Data, a practical guide which defines the notation, the rules and the specifications for the design, implementation and documentation of the Public Administration processes, documents and electronic data exchange messages.

The Interoperability Registry prototype, a web-based repository of service and document metadata, services process models in BPMN, standardized XML schemas for most commonly used governmental documents based on UN/CEFACT/CCTS standards, as well as codelists for the most common information elements within governmental service provision in Greece. It shall be noted that currently very few codelists have been added to the Greek eGIF.

The Greek eGIF is supplemented by conformance checklists that support the assessment of infrastructures against the framework and training material for Public Administration Officials and eGovernment Practitioners.

The administration of the Greek eGIF is proposed to be done centrally for all the Public Sector by the “Management Agency of the Framework” (Φορέας Διαχείρισης του Πλαισίου – ΦΔΠ). However, this authority has not yet been regulated and there are still negotiations for the management scheme among competent authorities.

Although electronic documents are not currently in common use in public administration, a few pieces of legislation are already in place regulating specific issues regarding electronic documents. In compliance with Directive 1999/93/EC on a Community Framework for electronic signatures, the
Presidential Decree 150/2001 was adopted. Recital 19 of the Directive provided that “electronic signatures will be used in the public sector within national and Community administrations and in communications between such administrations and with citizens and economic operators, for example in public procurement, taxation, social security, health and justice systems”. Consequently electronic signatures can be used in the frame of electronic documents in the context of eGovernment. Before the publication of P.D. 150/2000, the Greek legislator had foreseen the use of digital signatures in the frame of exchange of documents via electronic mail between public administration authorities or between them and the citizens in Article 14 of law 2672/1998. However electronic signatures were only defined in P.D. 150/2000.

Presidential Decree 342/2002 regulated which documents can be exchanged only when they bear a digital signature and which can be exchanged without one. According to Article 1 of P.D. 342/2002 decisions and certificates are exchanged via electronic mail among the authorities of the public administration, legal public entities, municipalities and local communities of Greece or between them and the natural or legal entities under private law, provided that they bear a digital signature. Furthermore, opinions, copies of minutes, proposals and reports are transferred via electronic mail from the authorities of the public administration, legal public entities, municipalities and local communities of Greece to the natural or legal entities under private law, provided that they bear a digital signature. The second article of the same P.D. states that the exchange of document via electronic mail without digital signature is allowed and valid among the authorities of the public administration, legal public entities, municipalities and local communities of Greece or between them and the natural or legal entities under private law, when it is not linked with the creation of legal results or with the exercise of a right, especially when their content relates to questions, circulars, instructions, studies, statistical data, requests for the provision of information and relevant answers.

Moreover, Article 20 of law 3448/2006 regulates terms and conditions for the provision of certification services from public administration bodies, which offer digital certificates for the provision of public sector services via the Syzefxis system or other public communications networks.

---


311 Article 14 “Exchange of documents via electronic means (facsimile – electronic mail)” of law 2672/98 (GG A’ 290) [Άρθρο 14 «Διακίνηση εγγράφων με ηλεκτρονικά μέσα (τηλεομοιοτυπία - ηλεκτρονικό ταχυδρομείο)» ν. 2672/98 ΦΕΚ Α’ 290.]


313 Law 3448/2006 on the re-use of public information and regulation of further issues of the Ministry of Internal Affairs, Public Administration and Decentralisation, GG A’ 57/15.03.2006) [Νόμος 3448/2006 για την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα και τη ρύθμιση θεμάτων αρμοδιότητας Υπουργείου Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, ΦΕΚ Α’ 57/15.03.2006].

14.1.2 Electronic documents for the purposes of the implementation of the Services Directive

The need for further changes in the existing eGovernment system in order to comply with Article 8 of the Services Directive (Directive 2006/123/EC) is explicitly admitted in the “Interoperability and electronic services provisioning framework” (hereafter “PDYHS”)315. In order to be able to fully comply with the obligations of Article 8 of the Services Directive there is a need for the adoption of new provisions and legislative instruments, which shall aim at the simplification of the procedures in the Public Sector and the implementation of the Community law into the Greek reality.316

The Greek eGovernment Interoperability Framework (Greek eGIF), and more specifically the PDYHS, aim at defining common standards and specifications for the design and implementation of information systems of public administration bodies, which support the provision of electronic services to other public administration bodies, enterprises and citizens, as well as the interoperability among them. The PDYHS also defines the general principles that need to be respected at both organisational and functional level, in order to be able to cooperate and exchange documents and information with other public bodies in order to offer complete electronic services to the citizens and enterprises317.

The information and data that are stored on the systems of a public administration body and relate with electronic services that are offered via public administration sites and portals shall be able to be exported into XML format.318 With regard to electronic documents PDYHS has chosen for the use of Standard XML schemas, which are further divided into three categories:

a. Horizontal XML standards (participating in general or sectoral services)
b. Sectoral XML standards (participating only in sectoral services)
c. International XML standards.319

In order to protect the data that exist in the Framework and to resolve the authentication problem, the PDYHS is suggesting the following measures320:

316 PDYHS, p. 23
317 PDYHS, p. 8
319 PDYHS, p. 56
320 PDYHS, p. 85-86
- **Public Key Infrastructure (PKI):** the Ministry of Internal Affairs has already started working on the necessary infrastructure for the application and use of electronic signatures\(^{321}\), in the frame of the Syzefxis project\(^{322}\), which is already functional. Moreover in the frame of the project "National Central Internet Gateway – Hermes" (Εθνική Κεντρική Διαδικτυακή Πύλη – ΕΡΜΗΣ) a corresponding Public Key Infrastructure is foreseen for the electronic transactions between the citizens and the enterprises with public authorities. The Public Key Infrastructure ensures, among others, the authentication of citizens and enterprises in their transactions with the public administration.

- The **XML Signature** Specification\(^{323}\) (XMLDSig, XML-DSig, XML-Sig), which can represent the digital signature of XML documents or part of them and can resolve crucial issues for the achievement of secure web applications, the authentication of the sender of a message of an internet service and the integrity of the data, in combination with additional requirements for keys, cryptographic algorithms, processing and interpretation of messages.\(^{324}\)

All the electronic services that are currently offered by the Greek public administration use as identification and authentication method the combination of usernames and passwords. This method does not sufficiently take into account the importance of the services and the possible implications in case of a security incident. The Digital Authentication Framework (herafter “PCA”\(^{325}\)) contains rules and instructions for the classification of the importance of every electronic service and consequently the choice of the authentication mechanisms.\(^{326}\) Annex B’ of the PCA contains the Digital Certificate Policy Framework, which specifies all the necessary procedures for the issuing, distribution and revocation of various types of digital certificates that can be issued according to the PCA. It also specifies the relevant audit procedures for the compliance of the digital certificate policies and the rules regarding the issuing of digital certificates by Certification Authorities.

According to the X.509 standard, a Digital Certificate Policy is considered “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements”. A Digital Certificate Policy, in general, is a useful tool for the user of PKI in order to decide whether a specific digital certificate is trustworthy to be used for a specific application. The PCA complies with the de facto standard RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, successor of RFC 2527.\(^{327}\) Annex C\(^{328}\) contains details about the Sectoral Digital Certificates.

The Interoperability Registry Prototype (Μοντέλο Τεκμηρίωσης) contains the documentation for the procedures, the documents and the XML schemes that will be modelled and designed for the needs of the Greek eGovernment project (eGIF). The Registry Prototype is based on the specifications and the

\(^{321}\) See also PD 150/2000


\(^{323}\) [XML-Signature Syntax and Processing](http://www.w3.org/TR/xmldsig-core/)

\(^{324}\) [PDYHS, p. 120](http://www.e-gif.gov.gr/Portals/0/eGIF_PCA_v2.pdf)

\(^{325}\) Πλαίσιο Ψηφιακής Αυθεντικοποίησης, έκδοση 2.00, May 2008, available online at [http://www.e-gif.gov.gr/Portals/0/eGIF_PCA_v2.pdf](http://www.e-gif.gov.gr/Portals/0/eGIF_PCA_v2.pdf)

\(^{326}\) PCA, p. 15

\(^{327}\) For more detailed information, see PCA, Annex B’ p. 119 ff.

\(^{328}\) For more detailed information, see PCA, Annex C’ p. 141 ff.
model prototypes that have been laid by international organisations, such as the World Wide Web Consortium (W3C), the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and the Object Management Group (OMG).\footnote{For more detailed information, see The Interoperability Registry Prototype, Μοντέλο Τεκμηρίωσης, Έκδοση 2.00, May 2008, available online at http://www.e-gif.gov.gr/Portals/0/eGIF_Montelo_Tekmiriosis_v2.pdf}

During March 2006 the Hellenic Public Administration Root Certification Authority (HPARCA) was established\footnote{Law 3448/2006, G.G. A' 57/15.03.2006}, and on the 10th of November the HPARCA Certification Practices Statement\footnote{GG B' 1654/10.11.2006} was issued. The HPARCA agency belongs to the Ministry of Interior and is the primary certification authority, responsible for the definition of policy and coordination of other public agencies that provide certification services. The establishment of a unique root certification authority for defining certificate policies and standards shall minimize interoperability issues.

In addition, according to the ‘SYZEFXIS’ project, the following five Certification Authorities will be established and will be subordinated to HPARCA:

- Ministry of Interior Certification Authority CA
- Ministry of National Economy and Finance CA
- Ministry of Health and Social Solidarity CA
- Ministry of Public Order CA
- Ministry of National Defence CA

At the moment the appropriate ministerial decisions are prepared for the establishment of the CAs\footnote{Note: The Ministry of Interior CA has at this point already been established (through Ministerial Decision/government gazette ΦΕΚ445/B/02-04-2007).}. This mechanism does not issue SSL certificates. The SSL certificates are signed by the VeriSign Inc.

The new infrastructure will link, rather than replace, all the back-office systems integrated by the several Public Administration Agencies.

The development of the National Authentication System will enable interoperable, digital transactions of all types, will save considerable financial resources to the Government and – the most important – will stimulate the evolution of the Public Administration from a group of independently operating Agencies to a network of interoperable and collaborative Public Services that are communicating constantly, with obvious benefits for the citizens and businesses\footnote{http://www.eppractice.eu/document/3368}.

The project “National Central Internet Gateway – Hermes” (Εθνική Κεντρική Διαδικτυακή Πύλη – ΕΡΜΗΣ) deploys a number of different authentication methods to deal with the diversity of the...
corresponding requirements of various eServices, ranging from the traditional use of username-password to the strongest method of digital certificates combined with the use of smart cards.

“Hermes has established a Certification Authority (CA), which has undertaken the task of issuing digital certificates to citizens and businesses for the purposes of authentication, digital signatures, and confidentiality. This CA is part of the Greek Public Sector Public Key Infrastructure (signed by the Hellenic Public Administration Root Certification Authority) which was established in the context of the SYZEFXIS project, the Greek Public Sector Network.

Not all government e-services however, are served by Hermes. The existing governmental sites continue to provide old as well as newly deployed services from their own sites. eGIF framework compatibility requires service providers to upgrade their authentication methods, if necessary, and be able to handle digital certificates. The latter is also necessary for the handling of digital signatures on electronic documents.

To promote interoperability of the certification services provided by Hermes CA and ensuring the wide acceptance of the issued certificates by all government bodies, several issues had to be considered originating mainly from the participating entities’ needs. The lack of a unique national ID for Greek citizens and the fact that most government departments identify citizens using sector IDs issued by them is just one of these issues.

The lack of unique national IDs and the restrictions imposed by the legal framework regarding private data protection had become the bottleneck at deploying digital certificates accepted by all government bodies. As a result, sector IDs had to be included in the certificate in an encrypted form and provided to authorised parties only under the user’s consent.

Citizens or businesses that wish to make use of the provided e-services that require strong authentication have to obtain from Hermes CA three different digital certificates:

• **Certificate for Digital Signatures and Authentication.**
  This certificate, when issued with a smart card, can be used for qualified electronic signatures based on the EU Directive 1999/93/EC.

• **Certificate for Encryption.**
  This certificate is used for providing confidentiality on exchanged data and documents.

• **Special Purpose Digital Certificate.**
  This certificate is used for conveying sector ids in encrypted form.

  These three certificates are “bound” together by the use of a common, yet unique to each certificate holder “Certificate Administration Code”.

  The Hermes certification services are complemented by the issuance of certificates to all civil servants for the purposes of performing their duties in a secure manner. More specifically, civil servants that
communicate data and handle documents are issued with two digital certificates (one for qualified electronic signatures and authentication and one for encryption)."\(^{334}\)

There are currently no plans regarding electronic documents from other Member States and EEA (European Economic Area) Countries. Due to the language particularities in Greece, currently all documents, which are going to be used officially, need to be officially translated by the Translation Department of the Ministry of Foreign Affairs or by designated and authorised lawyers.

It has been decided that the existing Citizen Service Centres ("KEP")\(^{335}\) will be made into Points of Single Contact. The Citizen Service Centres offer already a number of services online (see below “Criminal Records”) and have the infrastructure to offer electronic documents. The Citizen Service Centres portal handles approximately \([1.000]\) services out of about \(2.500\) Public Administration (PA) services. More than \(10.000\) organizations from Ministries to Municipalities and Prefectures are involved in the provision of those services and around \(4.000\) documents are exchanged in their context. The Citizen Service Centres Internet portal receives around \(230.000\) visits per month with about \(1.000.000\) visited pages. Its operation is supported by more than \(1,000\) Citizen Service Centres spread around Greece and linked together by a VPN network. Currently one of the problems in the process of offering electronic documents is the secure authentication of the user (citizen), which is currently being dealt with in the Greek e-Government Interoperability Framework, as has already been elaborated above.

14.2 Specific document types

14.2.1 Extracts from commercial registers

Extracts from the commercial registers are not offered electronically yet. However steps have already been taken in this direction. Law 3419/2005\(^{336}\) introduced the creation of the General Electronic Commercial Register, which will include all commercial actors, i.e. most types of companies and natural persons acting as merchants. It shall be noted that although the General Commercial Register was foreseen to start functioning before the 01.01.2007, it is not operational yet. Currently 29 chambers provide various certificates electronically through the Citizen Service Centres (KEPs). A political decision is still needed in order to provide these services on the Internet. For the time being the initial registration to the chambers is not offered electronically or through KEPs.


\(^{335}\) www.kep.gov.gr (Κέντρα Εξυπηρέτησης Πολιτών – Citizen Service Centres)

A unique registration number (Αριθμός Γενικού Εμπορικού Μητρώου) will be allocated to each registered entity or person, which will be available in documents issued by the General Electronic Register. According to Article 16 of Law 3419/2005 every interested party will be able to ask electronically or after submission of a paper application for certificates. The certificates can be provided, according to the preferences of the applicant, in paper or electronic format, if they concern registrations made after the 01.01.2007. However, as already mentioned, although the creation of the General Commercial Register was foreseen for the beginning of 2007, it is still not operational. In reality it may take years until the Register is operational, due to objections raised during the awarding procedure.

14.2.2 Criminal records

The citizens can request and obtain the extracts from the penal register (“αντίγραφο ποινικού μητρώου”) from the authorities themselves or at the Citizen Service Centre (KEP)337. The application can be made either electronically via the KEP website, either by phone (at the hotline of the Citizen’s Service Centres 1500) or directly by the citizen at a KEP physical office. In case the application is made electronically, the citizen can pick it up from a preferred KEP office. This choice is promoted, as the use of a username and password, used for the sending of the electronic application is considered as a weak authentication method, and therefore the physical presence of the applicant is also still needed for the collection of the paper. In any case the extract from the penal register will be delivered in paper form and not electronically.

The Ministry of Justice in cooperation with the “Information Society S.A.” programme have launched a new project on the “Establishment of Information Systems and Modernisation of the Penal Registry Services of the First Instance public prosecutor’s offices of six cities – Athens, Piraeus, Thessaloniki, Patras, Heraklion, Volos”338. In the frame of this project the Ministry of Justice has created a specific web page for the Penal Register, where the citizens can also find the application for the request of an extract from the penal register online, and where more information is available (http://www.ypiresiespoinikoumitroou.gr). Currently the online service is only available for the Athens Penal Registry Service. In the context of the same project some KEP offices can be connected and retrieve electronically the extract for citizens that fall under the Athens Penal Registry.

In 2005 the ex-officio request of the extracts from the penal register from public authorities was introduced. In compliance with law 3242/2004339, the joint Ministerial Decision nr. 2458/2005340 was adopted by the Under secretary of the Minister of the Internal Affairs, Public Administration and Decentralization and the Minister of Justice on the ex-officio request for the negative or positive declaration in replacement of the physical type of the extract from the penal register. The pure notification of the negative or positive declaration regarding the penal register condition of a citizen to the public authority that requested it ex-officio was not successful in practice (as a simple “yes” or

337 www.kep.gov.gr (Κέντρα Εξυπηρέτησης Πολιτών – Citizen Service Centers)
338 Εγκατάσταση Πληροφοριακών Συστημάτων και Εκπαγχρονισμός Υπηρεσιών Ποινικού Μητρώου Εισαγγελιών Πρωτοδικίων εξ (6) πόλεων - Αθήνα, Πειραιάς, Θεσσαλονίκη, Πάτρα, Ηράκλειο, Βόλος
339 «Ρυθμίσεις για την οργάνωση και λειτουργία της Κυβέρνησης, τη διοικητική διαδικασία και τους Ο.Τ.Α.» GG 102/A'/24-05-2004
340 GG 267/B'/01-03-2005
“no” was not sufficient to cover fully all requests) and was abandoned. A new Ministerial Decision amended the previous ones and modified the procedure for the ex-officio request of the extract from the penal register. The ex-officio requests can be submitted either via fax or via electronic mail and the relevant extracts from the penal register as sent back to the authorities via fax.

14.2.3 Extracts from professional registers

Professional registers are typically issued by private entities. Although it is not easy to create a complete overview of all professional registers, it appears that the extracts issued by such entities are commonly issued in paper form. The Technical chamber of Greece provides a number of certificates electronically through its website (www.tee.gr), which can also be provided by the KEP portal. From legal point of view is the same as the IKA certificates case, which is further analysed below (under certificates of insurance). Currently, no plans exist to make the use of electronic documents mandatory or to encourage them further.

As already mentioned above (under extracts from commercial registers), Law 3419/2005 has foreseen the creation of a General Commercial Register (electronic). The introduction of the General Commercial Register is expected to abolish the obligation for registration to Professional Chambers or that such registration would play a secondary role.

14.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form, but rather the insurer receives a paper copy or at most a scanned copy sent by fax.

Currently, an attempt to provide social insurance certificates electronically is realised by the Social Insurance Institute (Ινστιτούτο Κοινωνικών Ασφαλίσεων - ΙΚΑ). This service is offered in compliance with the Ministerial Decision of the Minister of Labour and Social Insurance on the “Provision of social insurance certificate via electronic communication”. According to the Ministerial Decision, the employers who are certified at IKA for electronic submission of their Analytical Periodical Statement (Αναλυτική Περιοδική Δήλωση – ΑΠΔ) have the opportunity to ask and receive electronically their

342 See www.ika.gr
344 Ministerial Decision on the terms and conditions for the submission of the Analytical Periodical Statements via the internet, Action Sheet 21/fln.2739/23.01.2002 (GG Β 87/2002) [Υπουργική απόφαση του Υπουργού Εργασίας και Κοινωνικών Ασφαλίσεων «Ορισμένα και προϋποθέσεις υποβολής...»]
social insurance certificate. The same opportunity to ask and receive electronically social insurance
certificates is given to specific entities and authorities\(^{345}\) (Citizen Service Centres, banks, notaries,
public authorities,…) that are certified or are entitled to be certified for the receipt of social insurance
certificates via fax, provided that they will register for the electronic services of IKA\(^{346}\). These services
are also provided through the KEP Offices by electronic means.

The social insurance certificate that is provided electronically bears a mechanical imprint of the
signature of the Head of the Informatics Department of IKA, as well as mechanical imprint of the
stamp of the office and is a public document (Article 2§1 of the Ministerial Decision). The
communication between the interested party and the special electronic service of IKA is realised via
personal passwords and passes for the modification of elements and communication\(^{347}\) (Article 3§1 of
the Ministerial Decision). So actually in this procedure there is an issue of authentication of the user of
the service.

Currently, there is also a proposal that the documents (certificates etc.) that are produced by an
electronic system are valid provided that the data entry has been approved and the system is working
according to the predefined specifications. This proposal, however, has still not been validated by law,
but it is expected to be validated by law in the near future.

### 14.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of
qualifications: generally, these are private sector issued documents for which only paper originals are
available. While electronic copies might occasionally be presented in the form of unsigned scans, this
is merely a matter of convenience.

\(^{345}\) A list of these entities and authorities can be found in Article 1§2 of the Ministerial Decision on the
provision of facsimile to certified at IKA entities, authorities and persons, for social insurance
certificate of the parties that transact with them, Action Sheet 11321/12490/878/24.07.2003 (GG B’
1138/2003) [Υπουργική απόφαση του Υπουργού Εργασίας και Κοινωνικών Ασφαλίσεων «Παροχή
ηλεκτρονικούς προς πιστοποιήμενους στο ΙΚΑ φορείς, υπηρεσίες και πρόσωπα, για βεβαίωση
ασφαλιστικής ενημερότητας συναλλασσόμενου με αυτούς», Φ. 11321/12490/878/24.07.2003 (ΦΕΚ Β’

\(^{346}\) The procedure in order to register for the electronic services of IKA is described in Ministerial
Decision on the terms and conditions for the submission of the Analytical Periodical Statements via
the internet, Action Sheet 21/fi3.2739/23.01.2002 (GG B 87/2002) [Υπουργική απόφαση του Υπουργού Εργασίας και Κοινωνικών Ασφαλίσεων «Όροι και προϋποθέσεις υποβολής Αναλυτικών
Περιοδικών Δηλώσεων (ΑΠΔ) μέσω διαδικτύου, Φ21/οικ.2739/23.01.2002 (ΦΕΚ Β 87/2002)].

\(^{347}\) The passwords and pass codes are provided to them by IKA, according to the procedure foreseen
in Ministerial Decision on the terms and conditions for the submission of the Analytical Periodical
14.2.6 Statements from the service provider

To our knowledge, there are currently no statements made by the service providers themselves fully electronically. Currently a number of documents can be submitted by the service providers in simple copy, without the need to officially certify the copy. A simple declaration from the service provider that the documents are genuine is enough. In the future it would be possible to integrate such statements on the website of the Points of Single Contact, but no such choice has been made yet.

14.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

14.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As already described above, the Greek eGovernment Interoperability Framework defines standards, specifications and rules for the development and deployment of web-based front and back office systems (including the creation and exchange of electronic documents) for the Greek Public Administration, at national and local level, which will accelerate the development of electronic collaboration of public agencies, for the delivery of high quality and secure one-stop eGovernment services to businesses, citizens and other public bodies.

As already mentioned above, the Digital Authentication Framework (PCA)\(^{348}\) contains rules and instructions for the classification of the importance of every electronic service and consequently the choice of the authentication mechanisms.\(^{349}\) The same document contains the Digital Certificate Policy Framework, which specifies all the necessary procedures for the issuing, distribution and revocation of various types of digital certificates that can be issued according to the PCA. It also specifies the relevant audit procedures for the compliance of the digital certificate policies and the rules regarding the issuing of digital certificates by Certification Authorities. This procedure will be used to support the provision of electronic services to other public administration bodies, enterprises and citizens, as well as the interoperability among them. So, this will probably also be used so that the public administration bodies will send replies and documents to the service providers through the Point of Single Contact. However, it shall first be defined who will play the role of the Points of Single Contact, as required by the Services Directive, in order to be able to have more detailed information about the “back office” and how the service provider will no longer have to correspond with any other entity that the Point of Single Contact.

\(^{348}\) Πλαίσιο Ψηφιακής Αυθεντικοποίησης, έκδοση 2.00, Μαΐου 2008, available online at \textcolor{blue}{http://www.e-gif.gov.gr/Portals/0/eGIF_PCA_v2.pdf}

\(^{349}\) PCA, p. 15
14.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Currently, the Citizen Service Centres\(^{350}\) have multiple physical establishments across Greece as well as a centralised website. The website offers a lot of information electronically, as well as online applications, webforms etc. As already mentioned above the Citizen Service Centres are already very close to what the Services Directive defines as Point of Single Contact, but still faces a major issue regarding the authentication of the user (citizens or enterprises). This is expected to be resolved after the implementation of the Greek eGovernment Interoperability Framework in conjunction with the Syzefxis project and the Hermes portal (see below).

More detailed rules regarding the use of specific languages, options for delivery of information etc. are still to be defined. With regard to communication with the service provider, no specific final decisions have been made at this point yet. Currently the Hermes and the KEP portal provide the information in Greek, English, French and German. Furthermore, according to the Greek eGIF all the appropriate metadata (tags etc.) will be in English for interoperability reasons.

In any case, the procedures will probably be facilitated by the creation of the Electronic Commercial Register\(^{351}\), which will include all commercial actors, i.e. most types of companies and natural persons acting as merchants. A unique registration number would be allocated to each registered entity or person, which will be available in documents issued by the electronic register. However it is not known when the creation of the Electronic Commercial Register will be completed, as it was initially foreseen for the 01.01.2007.

14.4 Assessment – Plans, progress and proposals for further harmonisation

14.4.1 Current plans and progress in the implementation of the Services Directive

As shown in the overview above, Greece has recognised the need to make significant efforts in order to comply with the provisions of the Services Directive and mainly with Article 8. In order to be able to fully comply with the obligations of Article 8 of the Services Directive there is need for the adoption of new provisions and legislative instruments, which shall aim at the simplification of the procedures in the Public Sector and the implementation of the Community law into the Greek reality.\(^{352}\)

The Greek eGovernment Interoperability Framework has made specific and very detailed choices with regard to the standards, the procedures and the technologies required for the registration, identification and authentication of the eGovernment services users, including citizens, businesses,

\(^{350}\) www.kep.gov.gr

\(^{351}\) Law 3419/2005, see above

\(^{352}\) PDYHS, p. 23
public authorities and civil servants. It also aims at creating an integrated and coherent set of policies, regarding Digital Certificates and Public Key Infrastructures.

The Interoperability Registry Prototype (Μοντέλο Τεκμηρίωσης), which contains the documentation for the procedures, the document and the XML schemes that will be modeled and designed for the needs of the Greek eGovernment project (eGIF), is based on the specifications and the model prototypes that have been laid by international organisations, such as the World Wide Web Consortium (W3C), the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and the Object Management Group (OMG). With regard to electronic documents the eGIF has chosen for the use of Standard XML schemas.

In order to protect the data that exist in the Framework and to resolve the authentication problem, the eGIF is suggesting the use of Public Key Infrastructure (PKI) and the XML Signature Specification (XMLDSig, XML-DSig, XML-Sig). The eGIF also specifies all the necessary procedures for the issuing, distribution and revocation of various types of digital certificates that can be issued according to the Digital Authentication Framework.

Besides the Greek eGovernment Interoperability Framework, the Syzefxis project is of great importance. The Syzefxis project aims at the improvement of public services’ functions supported by the upgrade of telecommunications infrastructure between them through the offer of advanced and low cost telematics and at the provision of integrated services to citizens using modern and user friendly government information and transaction systems. Via this project PKI technology will be broadly used in the public sector, facilitating the broader use of electronic signatures. “The use of electronic Signatures and cryptographic services will ensure secure data exchange and electronic transactions, initially, among public administration bodies. The mentioned services will be set up on top of the Public Key Infrastructure (PKI), the most reliable technology in this area, provided by the National Public Administration Network ‘SYZEFXIS’. In this context 50.000 smart cards (accompanied by 10.000 pertinent card readers) are distributed to civil servants. Smart cards contain two digital certificates, respectively used for electronically signing and ciphering documents. Their distribution and use, governed by federal, regional and local laws, will minimize any interoperability difficulties between the public sector agencies and their prospective applications”.

The project National Central Internet Gateway – Hermes (Εθνική Κεντρική Διαδικτυακή Πύλη – ΕΡΜΗΣ) is an ongoing project which aims at the creation of the Central Greek Public Sector portal that will offer complete and secure eGovernment services via a central eGovernment portal, known as National Portal “Hermes”. The projects aims also at the creation of the necessary infrastructure for the provision of electronic transactions with the Public Administration, as well as the digital authentication of citizens and enterprises, in order to support in a secure, reliable and efficient way the access of the citizens and enterprises to various eGovernment services, offering authentication, digital signature and cryptography services, and in general the necessary protection to the citizens and the enterprises when interacting on the internet. The Digital Authentication service will ensure not only the electronic transaction services that will be deployed within the Hermes project, but also services that are already

353 For more detailed information, see The Interoperability Registry Prototype, Μοντέλο Τεκμηρίωσης, Έκδοση 2.00, May 2008, available online at http://www.e-gif.gov.gr/Portals/0/eGIF_Montelo_Tekmiriwsis_v2.pdf
354 XML-Signature Syntax and Processing (www.w3.org/TR/xmldsig-core/)
or will be offered in the future by third public entities. It shall also be noted that the project aims at the creation of a trusted third party and includes the provision of Digital Authentication services exclusively via the infrastructure of the Ministry of Internal Affairs. 

Hermes is designed to provide the operations that are necessary for the delivery of e-services from a single point of contact. Hermes will also host the Greek eGIF Interoperability Registry and the consultation and deliberation mechanism for the evolvement of the Greek eGIF. (For the authentication methods used in Hermes, see above, section “Electronic documents for the purposes of the implementation of the Services Directive”.

“Initially it has been verified that more than 250 authorities can provide content that can be of interest to the users of Hermes. These authorities have been categorized based on the following criteria:

- The content volume
- The audiences that are served by these authorities; niche audiences are not excluded, but they are characterized as low priority publics
- The frequency of content updating.

According to these criteria three groups of authorities have been identified:

- Crucial public administration authorities, the content of which is very important for Hermes
- Important public administration authorities, the content of which is relatively important
- Indifferent public administration authorities; the content is less important

Of course it is recognized that the level of an authority can change over time and it is important to monitor the performance of the authorities based on these criteria. The overall effort is enhanced by the measurements of the public interest as occurring by the Management Information System of the Citizen Service Centers (KEP), which provides insight on the public interest in a dynamic fashion.

In parallel to selecting the preferred authorities, we have to deal with the important technical issue of content provision from multiple sources. Manual, semi-automated and automated (web services, RSS) ways have been explored.

- Content and metadata insertion on behalf of the third-party authorities, using forms
- Retrieval of content and metadata on behalf of the Hermes system, invoking the web services provided by the authorities
- Provision of content and metadata on behalf of the authorities invoking the web services provided by the authorities.

Hermes has thematically organized all service and content areas. This organization is based on three criteria:

---

eDocuments and e-Delivery
in the context of the services directive
Country Profiles report

• The Government Category List (GCL)
• The users
• The government authorities

This way a set of metadata has been created that support the – to a certain degree – automatic categorization of new content. All ways of content provisioning (from the manual to the automated) enforce the usage of metadata. All tasks are supported by a well defined workflow engine.

In the context of the Hermes project, a national Interoperability Registry is being implemented, which will be ‘a web-based repository of service and document metadata, services process models, standardized XML schemas for mostly used governmental documents based on UN/CEFACT/CCTS standards, as well as codelists for the most common information elements within governmental service provision in Greece’.

In practice, the front end is computerized to a significant degree, i.e. the citizens and business can invoke a set of services using the web forms of the KEP’s portal; however the back office, i.e. the execution of the service itself as well as the delivery of the result are performed to a significant degree manually. Hermes is extending the computerization to the back office allowing the service execution to take place in a fully electronic fashion. As expected adaptation of the legislation framework and organizational changes is required.

The concept of the Citizen and Business Certification Registry (or “document safe” as it appears in other European implementations) was an idea that we have explored. Although it was expected to offer significant benefits for the integration and collaboration of the IS in the Public Sector we have met difficulties in terms of the legislation and objections coming from the Hellenic Data Protection Authority.

Non-repudiation is a significant issue in the content of service provision. For this purpose, a Time Stamping server is deployed, which is expected to play a significant role in the provision of e-gov services at both ends (inbound request coming from the citizen/business and outbound response returning to the citizen/business) and potentially in the individual steps (especially when different agencies are involved).\(^\text{357}\)

14.4.2 Suggestions for further European support initiatives

The Interoperability Registry Prototype (Μοντέλο Τεκμηρίωσης) is based on the specifications and the model prototypes that have been laid by international organisations, such as the World Wide Web Consortium (W3C), the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and the Object Management Group (OMG).\textsuperscript{358} With regard to electronic documents the eGIF has chosen for the use of Standard XML schemas. However, more detailed specifications mandated by the European Union would be definitely beneficial for the interoperability of the systems and the exchange of information and documents between the Member States.

Although the eGIF project contains detailed information about the Digital Certificates and the Syzefxis and Hermes project further define the use of PKI in Public Administration, it is not self evident that the system will be interoperable with all certificates created in another Member State.

At any rate, key difficulties in practice include the determination of the reliability and responsibilities of Certification Service Providers of other Member States, and the ownership of these CSPs, as it may be politically sensitive to support CSPs which are not under public sector supervision. Thus, the issue of electronic signature support is certainly a field where European initiatives could be useful in order to improve trust or facilitate validation of electronic signatures.

\textsuperscript{358} For more detailed information, see The Interoperability Registry Prototype, Μοντέλο Τεκμηρίωσης, Έκδοση 2.00, May 2008, available online at http://www.e-gif.gov.gr/Portals/0/eGIF_Montelo_Tekmiirisis_v2.pdf
15 Hungary

15.1 General framework for electronic documents in eGovernment applications

15.1.1 Electronic documents in eGovernment applications

In Hungary, the Governmental Portal\textsuperscript{359} developed since 2003 insures the usage of eGovernment applications by the means of the Central Electronic Service Provisioning System (hereafter: CESPS). The Client Gate is the entry point for natural persons or for undertakings/services and the Office Gate for the data transmission inside of the public administration on the CESPS\textsuperscript{360}.


It is a requirement of Ket for the electronic administration, that the electronic documents shall be signed at least with an advanced electronic signature\textsuperscript{361}; however this is not necessary in the case of submission through the Client Gate. The use of the Client Gate is linked to a prior face to face registration. Any natural person (including foreigner citizens) may apply for her/his client gate accesses (more than one at the same time) via an electronically signed form using at least advanced electronic signature or personally in one of the 274 Document Bureaus. It is currently planned to eventually include foreign representations of Hungary as points of registration as well. There is a Central Document Bureau operated by the Central Office for Administrative and Electronic Public Services (Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala (hereafter: KEKKH\textsuperscript{362}) in Budapest. The personal data and the e-mail address of the applicant are stored in a central database of the CESPS and are used for identification and authentication with the sectoral systems or using Certification Service Providers (hereafter: CSP) in a special authentication procedure, the so called reidentification process.

\textsuperscript{359} See http://www.magyarorszag.hu/english
\textsuperscript{360} Government Decree 182 of 27 July 2007 on the Central Electronic Service Provisioning System - 182/2007. (VII. 10.) Korm. rendelet a központi elektronikus szolgáltató rendszerrel
\textsuperscript{361} The certification authority should use face to face registration, etc. See later and the Gov. Decree 193 of 2005.
\textsuperscript{362} KEKKH 1094 Budapest, Balázs Béla utca 35. http://www.nyilvantarto.hu
CESPS authenticates users based on a user name and password. The electronic documents uploaded through the Client Gate will be signed and time stamped automatically by the CESPS. CESPS confirms the reception by a time stamped and electronically signed document sent to the client's e-mail address. A more detailed description of this system can be found in the Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications NATIONAL PROFILE HUNGARY April 2007; see http://ec.europa.eu/idabc/servlets/Doc?id=29085.

There are printable or electronically filled out forms downloadable from the Governmental Portal or from the web sites of authorities and local governments. A general electronic form designer and completion program is offered to the authorities by the CESPS. The issuing of electronic fill out forms is mandatory for the authorities from 31 March 2009. The first and widely used electronic applications are the electronic tax declaration program and the program used for electronic company registration.

The printable original forms especially which require or allow the identification of the user have to be printed out, signed and presented by the service provider in person to one of the Document Bureaus or in other cases to the client service bureaus of the competent authority operating electronic services (e.g. in case of tax, pension etc.) or sent via traditional mail. As mentioned above, the submission of the electronically filled forms (sent as an XML file) through the Client Gate does not require an electronic signature; however prior personal registration both on the Client Gate and the sectoral system is required.

The Secure Electronic Document Transmission Service (hereafter: BEDSZ), a service of the CESPS, ensures the transfer of documents between the Client Gate and the competent authorities (sectoral systems) and between the offices inside the public administration. For the initial use of the services of the sectoral systems (e.g. electronic tax declarations, authorization of a case assistant) a paper based declaration should be sent by traditional mail as noted above.

The network infrastructure of CESPS for the transmission of electronic documents is provided by the high speed, secure Electronic Governmental Backbone (hereafter: EKG). Joining the EKG for the central and territorial organization of the public administration, for law enforcement and for the Document Bureaus is compulsory; for other state budgetary organizations, public bodies and the local governments the joining is voluntary. Business organizations can join only if they provide public functions.

Act XXXV of 2001 on electronic signatures put the exclusive use of electronic documents in state administration procedures that is electronic administration from September 2001, under the jurisdiction of sectoral regulation, but made the acceptance of qualified electronic certificates compulsory both for court and public administration procedures.

Ket binds the acceptance of the qualified or advanced electronic signatures beyond the check of the signature's validity to the identity verification of the signer as well. The process of reidentification is prescribed for that. Any certificate, issued by any CSP of a Member State or EEA country providing reidentification may be accepted. The detailed requirements are regulated in the government decree 194 of 22 September 2005 on the electronic signature used in public administration procedures and the certifications thereof, and the requirements for the certification service providers issuing the certificates.
The Public Administration RootCA Hungary (hereafter: KGYHSZ) issues the issuer certificate for the Hungarian CSPs – both in public administration and in the business sector – which comply with the criteria provided for in the legislation. The National Communication Authority keeps a register on the certification policies conforming to the criteria for the use in the public administration and on CSPs operating under those policies. Upon request of a Hungarian public administration authority any CSP with establishment in the European Economic Community can be entered into this register in case of legal and interoperability compliance.

KGYHSZ can issue trusted lists (TSL) and can join to the European Bridge CA planned earlier in the IDABC program.

Further technical requirements are prescribed in the following:
- On the security, interoperability and uniform use of IT systems in electronic administration (Government decree 195 of 22 September 2005.)
- On the detailed technical rules for documents in electronic administration (Decree of IHM 12 of 27 October 2005.)
- On the rules of replicating paper based documents into electronic format (Decree of IHM 13 of 27 October 2005.)
- On the rules of electronically conducted tax cases (Decree of PM 34 of 29 December 2007.)

According to the legislation the character mode formats of electronic documents are:
- ISO/IEC 646:1991 (7 bits, ASCII character set for information exchange purposes)
- ISO 8859-1:1998 (Latin-1, 8 bits graphical character set)
- ISO 10646:2003 (Unicode v.4.0)

Text and image formats:
- Microsoft Rich Text Format 1.7.
- Portable Document Format 1.3.
- (Tiff image files may be attached to tax form sheets)

Format of e-mail message and format of text and non-text content sent using e-mail services:
- IETF RFC 2822 (Internet Message Format)
- IETF RFC 2045 (Multipurpose Internet Mail Extensions, MIME)

The required formats of electronic signatures are regulated in three recommendations of the former Ministry of Informatics and Communications (IHM) issued in 2005. (http://www.itktb.hu/engine.aspx?page=dokumentumtar in the subdirectory: ELKA-MEKIK), and there is a decree of the minister of justice concerning the electronic company register, with the same format regulations. (Decree of IM 24, 18 May 2006 on some questions of electronic company registration process and registration)

Electronic signature formats: ETSI TS 101 903 XAdES-T, XAdES-C, or XAdES-A respectively
Time stamping: according to RFC 3161 and ETSI TS 101861 algorithm RSA, fingerprint SHA-1
Certificate profile formats: for the public administration: 14 certificate profiles were specified based on RFC 3280, RFC 3739 and ETSI TS 101862.

15.1.2 Electronic documents for the purposes of the implementation of the Services Directive

The usage of electronic documents depends on the Hungarian electronic administration applications. It is clear that the development objectives of the applications do not meet the requirements of the Service Directive in every instance; however, the Client Gate and the applications of the existing public administration infrastructure may yield the basis for the technical realization of the Service Directive. The legal and organizational questions constitute a more considerable problem for the transposition.

The already cited regulations in the previous section do not make a distinction based on the country from which the Client Gate is accessed. The requirements of electronic documents and electronic signatures are in accordance with international recommendations and standards. The registration and amendment notification processes of business associations with legal personality and of business associations lacking the legal status of a legal person are exclusively electronic. The Company Information Service of the Ministry of Justice and Law Enforcement, the County Courts of Registry and the members of the Hungarian Bar Association are using qualified certificates and time stamps of the commercial CSPs Netlock and Microsec. Service providers can use advanced certificates from any CSP that has been registered as noted above.

The data of the Company Register and the tax information systems are accessible online, however in company registration (amendment notification) proceedings legal representation is mandatory. The service provider business associations must engage the services of a lawyer for the company foundation and company registration processes as a case assistant, who is the member of the Hungarian Bar Association. The Company Information Service issues official copies of company records, certificates of incorporation and company certificates from the companies register as authentic electronically signed and time stamped electronic or traditional authentic paper documents upon request.

Generally the not too large undertakings entrust a third party accountant office not only with the bookkeeping, but with the electronic administration of taxes and social insurance contributions for the Tax and Financial Control Administration (APEH) and for the Tax Department of the competent Local Government, with the regular declaration the data of the employees for the National Health Insurance Found (OEP) or for the Central Administration of National Pension Insurance (ONyF), etc. The usage of all such sectoral systems requires personal paper based registration and/or authorization of the “case assistant” physically at the service bureaus of the authority or by traditional mail. Afterwards, almost all of these systems can be accessed through the Client Gate and the CESPS. There are downloadable fill-out programs, and some of them need electronic signatures and/or apply encryption.

363 See: Act V of 2006 on Public Company Information, Company Registration and Winding-up Proceedings
In Hungary, the administrative burdens of the undertakings are significantly higher than the average of the EU. The dissemination of the electronic administration and One Stop Shops, the reduction of the administrative time in half, and the establishment of client information centers are among the objectives of the current government program. More development programs have started to execute the government program, among them for the undertakings' support, and the reduction of administrative burdens. The most extensive program is the Hungarian e-Government 2010 Strategy and its related Program Plan. The Program contains the implementation of a service provider model based on users demands, the simplification of the processes, the data management supporting the services between the sectoral systems, and the realization of the information management as well in its overall programs based on 5 horizontal programs. An essential task is the standardization for the provision of interoperability of the connected information systems and databases.

There are several obstacles before the transposition of the Services Directive, which should be eliminated in the near future. For example: attested, official translations are necessary for foreign language documents, insofar as the language of the administration is Hungarian.

Private entrepreneurs, as one possible form of an undertaking without the status of a legal entity, can be only a natural person living in Hungary. A private entrepreneur's license is issued by the notary of the local government who is competent as determined by the residence of the undertaking. It is necessary to apply personally for the license and to accept it in person. The notary electronically registers the data of the entrepreneur. The centralized register of the private entrepreneurs is operated by KEKKH. One can obtain data from the public register of KEKKH through an application via a paper based request form. In contrast, the Company Register is operated by the competent county courts of registry, but it is nation wide integrated and searchable on-line.

The registration of business associations occurs at the courts of registry. The application for registration (amendment notification) shall be submitted in an electronic document to the court of registry of jurisdiction as determined by the company's registered office. The submission shall be made by the company’s legitimate representative through a legal representative (a member of a lawyer's office). The Hungarian Bar Association gives the certificate to its member lawyers necessary to obtain the technical tools and certificates of electronic signature from the CSP usable in the process of electronic company registration. To found a company, personal contact is necessary for the lawyer's commission, similar to the process for a private undertaking. A foreign country lawyer's office can be involved based through on a cooperation contract set with a Hungarian office.

The annual report of a company prepared in an electronic format must be sent by the company’s legitimate representative or legal representative, and the annual report converted into electronic format shall be sent by the legal representative by way of electronic means to the company information service for publication along with payment of publication charges. The report’s electronic format shall also constitute compliance with the obligation of deposit. The legal representative shall enclose his authorisation as well.

364 See on http://ekk.gov.hu/hu/ekk/strategia
365 Act V. of 1990 on the private undertaking; 1990. évi V. törvény az egyéni vállalkozásról
366 See http://www.magyarugyvedikamara.hu/?content=10x&scontent=1
It can be said that, based on the applicable regulations, use of the point of single contact or the overall electronic administration by service providers from other Member States was considered unavailable until the first half of 2008.

According to the Government decision 2055 of 9 May 2008 on the tasks deriving from implementation of the Services Directive, a compliance screening of the legal regulation took place. A schedule was made for the necessary modifications. There are about 500 cases of administration concerned by the Services Directive. For the realization of the requirements of the Services Directive a bill was being prepared about the regulatory framework and about the necessary law amendments.

Inter alia Ket and its executive decrees will be amended. After the necessary amendment of acts, the decrees of local governments not conforming for the new legality requirements shall be amended. It will be necessary to create general procedural rules related to the distributed jurisdiction practice of authorities in connection with the Ket amendment, to eliminate the legal obstacles of electronic communication caused by the procedural law between client and the authority, and between the acting authorities, especially to facilitate electronic communication and to ensure that clients may satisfy their payment liabilities with the competent authority.

For the implementation of Single Point of Contact (hereafter: SPC), a feasibility study, a concept, a schedule will be prepared defining the affected authorities to be involved and their role. The services provided by the SPC and the authorities, including offices to be contacted will be summarized in a guide for the service providers and clients. A separate study will be prepared on the function of the contact points providing the physical, personal contact. The necessary tasks will be defined to the forming of the Hungarian Internal Market Information (IMI) system structure.

In connection with these efforts, the Government decision 1058 of 9 September 2008 defines the governmental program initiated to reduce administrative burdens of market and non market players' and for the simplification and acceleration of administrative procedures. The use of electronic communication, “One Stop Shop” administrations, more flexible administrative obligations and more efficient treatment of data stored in authentic registers is included in the principles of the program. It should be assured by 2011 that the communication between the authorities happens overall and exclusively by electronic means in the administrative processes, with the exception cases which can be accomplished more efficiently by other means. Every form used in the public administration processes or in other processes of the state shall be downloadable from the Governmental Portal. The fill-out forms shall be based on a unified platform.

The creation of the legal basis for the establishment of points of single contact as required by the Services Directive is coordinated by the minister of justice and law enforcement. All services which can be employed by the undertakings for the fulfilment of requirements will be integrated in this framework. All procedures and formalities relating to access to a service activity and to the exercise thereof and relating the application for the licences relating to the exercise of their activity shall be integrated. Most of the tasks shall be finalized by the end of 2008. By this time the completion of the feasibility study on the implementation of the Services Directive is expected. The feasibility study shall define the form of PSC realization and all other requirements of the implementation.

Hungary is awaiting the necessary shaping of common trends and requirements for document types and acceptable electronic signatures at the European level for the startup of implementation.
Regarding the realization of single points of contact, there are two relevant nation-wide existing systems for the registration of service providers according to the legislation in Hungary. Firstly, the infrastructure of the Company Register managed by the 20 county registration courts and with many joined lawyer’s offices is used for business associations, and the 274 Document Bureaus with the KEKKH is used for private entrepreneurs. Through representation by a lawyer or competent notary of the district centre at the Document Bureau, a number of registration formalities must be fulfilled in person, including through the presentation of several documents (e.g. certificates of ‘no criminal records’, cheque or certificate of the fee paid, demonstrating technical capability through diplomas, licenses and permits, registering with professional bodies, etc). Most of these currently exist only in paper form. Currently the service provider can access none of these purely at a distance and by electronic means; however this concept could be a starting point for the reshaping in order to meet the requirements of the Services Directive.

15.2 Specific document types

15.2.1 Extracts from commercial registers

There are several ways to get electronic extracts from commercial registers in Hungary. The most recent solution is to use the website of the Company Information Service http://www.e-cegjegyzek.hu/info/page/ceginfo or through the Client Gate, since the Ministry of Justice and Law Enforcement made some company information accessible on-line for anyone free of charge as of 1 January 2008. The freely accessible information is:

- Company name,
- Seat of establishment,
- Address of company sites and branch(s);
- Company’s main business activity and the list of activities,
- Company’s subscribed capital;
- Tax number,
- Time of the opening and conclusion of dissolution proceedings,
- Time of the opening and conclusion of liquidation proceedings.

Prior to the general opening of this system to the users of the Governmental Portal by means of the Client Gate, there was no charge only if the volume of information requested remained below 15 searches per month.

The freely accessible company information is however informative only, and the information would not be usable as an authentic document.
The Company Information Service provides access free of charge\textsuperscript{367} to any data (current or previous) recorded in the companies register, and to any data contained in an application for registration (amendment notification) which are recorded electronically pending registration, to any party, if the request is submitted by way of electronic means. (http://ceginformaciosszolgalat.irm.gov.hu/?npmid=3).

If persons request any company information other than the information mentioned above or if they request company information in the form of an authentic official document, they shall be charged for using the services of the Company Information Service consistent with the costs of the service provided. The Company Information Service shall supply information to the court, the prosecutor’s office, an investigative authority or other administrative body, notary public, court bailiff, liquidator, to chambers of commerce and trade associations to the extent required for discharging their duties conferred upon them by law free of charge, including any data not mentioned above. These entities are required to reimburse the Company Information Service for the costs arising in connection with the use of the computer system only, provided that the request for company information was launched by way of electronic means.

The Company Information Service issues official copies of company records\textsuperscript{368}, as authentic electronically signed and time stamped electronic or traditional authentic official paper documents, or official electronic documents upon request.

The request shall be made personally, by traditional mail, by fax or by e-mail electronically signed at least with advanced electronic signature, except when the request is made by means of the Client Gate of the Governmental Portal. The members of companies can use advanced certificates from any registered CSP. The Hungarian CSPs are operating their services with OCSP. The Company Information Service verifies the certificates and handles the requests. The fee for electronic documents is lower than for paper forms.

If an agreement is concluded with the Ministry of Justice and Law Enforcement, the applicant can also access on-line the database of the company register on the network of the Company Information Service (https://occsz.e-cegjegyzek.hu/info/page/ceginfo) connecting the county courts of registry. There is a special free downloadable software (http://srv.e-szigno.hu/menu/index.php?lap=letolt) e-Szigno for the inspection of data.

The Company Information Service may deliver the following information upon request:

- Copy of company records;
- Certificate of incorporation;
- Company certificate;
- Business card of the company;
- Company name;
- Company information on the company documents sent by electronic means or company documents on paper converted into electronic format;

\textsuperscript{367} See 4 Article 15

\textsuperscript{368} See Decree of IM 24 of 18 May 2006 on some questions of the electronic process of company registration; 24/2006. (V. 18.) IM rendelet, az elektronikus cégbejegyzési eljárás és cégnyilvántartás egyes kérdéseiről
• Company information on the annual report in whole prepared according to the Accounting Act or a part of it (balance, statement of achievement, supplements);
• Company information on rulings of the court of registry or of other courts concerning the company;
• Company information on the text of every notices of courts of registry published in the Company Gazette;
• Examination of the records of the company register by electronic means;
• Company watching

Company Information Service sends the requested information to the e-mail address given by the applier in one of the following format:

- Authentic official electronic document. The official document is qualified as the Company Information Service signs with qualified electronic signature and is time stamped. The Authentic official electronic document sent is authentic only in electronic format.
- Official electronic document which do not contain qualified electronic signature and time stamp.

15.2.2 Criminal records

The certificate of the so called “proof of sound behaviour and mores” is an authentic official document issued from the records of the register of criminal cases. Having a certificate of 'no criminal records' is a condition for some posts of undertakings or for the issuing the license of private entrepreneurs. The concerned natural person may ask for it independently from her/his citizenship sending a filled and signed special paper form with the postal cheque on the payment of fee to the KEKKH. The paper form is available at the post offices as stationery. After the successful conclusion of the ePayment project electronic submission will also be made possible. The filled data shall be the same as in the personal identification documents of the applicant.

The Central Office for Administrative and Electronic Public Services (KEKKH) is authorized to issue the “proof of sound behaviour and mores” in Hungary369.

The “proof of sound behaviour and mores” is issued only in paper format and is valid until 3 months counting from the date of issuing. It may contain the note of 'no criminal records' or in the case of criminal conviction of the applier the data concerning the individual punishments and measures.

KEKKH sends the certificate by traditional mail to the address given on the application by the person.

369 See Act LXXXV of 1999 On the register of criminal cases and on authentic certificates “proof of sound behaviour and mores” and the Decree of BM 6 of 11 February 2000 on the authentic certificates of “proof of sound behaviour and mores”.

---

Version:.................... 1.3
Issued on: ................ 24-02-2009
15.2.3 Extracts from professional registers

A central and generally mandatory professional register doesn’t exist in Hungary.

There are chambers of trade and industry and several professional chambers on national, county and town level which maintain their own registers of members. Some of such registers can be accessed on the website of the chamber, but the extracts are in paper form.

The private professional or scientific bodies also provide attestations to their experts based on their own registers in paper form only.

The legal possibility to issue electronic extracts exists, due to the implementation of the signature act transposing the Signatures Directive, but in practice only paper documents are commonly required and issued.

Currently, no plans exist to make the use of electronic extracts of professional registers mandatory. The company register or the register of private entrepreneurs contain the same electronic information and are publicly accessible as was described in the previous section.

15.2.4 Certificates of insurance

Certificates of insurance are not issued in an electronic form. The legal possibility to issue electronic extracts exists, due to the implementation of the signature act transposing the Signatures Directive, but in practice only paper documents are commonly required and issued.

Currently, no plans exist to make the use of electronic certificates of insurance mandatory or to encourage them further.

---

370 See Act XXXV of 2001 on electronic signatures
15.2.5 Proofs of qualifications

The documents about the proofs of qualification shall be in paper form according to the legislation in force\textsuperscript{371}.

The issuing of certificates or diplomas exclusively in electronic format seems unlikely, however it is possible to copy them into an authentic electronic document, via the Hungarian Chamber of Civil Law Notaries\textsuperscript{372} which authenticates and issues the Apostille certificate of the translated documents necessary abroad.

It should be noted that the organizers of examinations shall send a protocol summarizing the results of the examinations in an electronic document signed with advanced electronic signature for the central register of vocational examination. The register is operated by the Registry Centre of the NSZFI (National Institute of Vocational and Adult Training), and the statistics of the quarterly results are available on-line\textsuperscript{373}.

15.2.6 Statements from the service provider

Statements made by the service provider himself for the authorities are sent through the Client Gate of the Governmental Portal via web forms to be completed.

The electronic document from the client (service provider) is transferred with encryption to the competent authority by the BEDSZ, a service of the CESPS. The encryption of documents happens on the client’s computer with the public encryption key of the recipient authority. The public encryption key of the recipient authority is delivered with the downloaded web form. The document is encrypted by the form filler program.

As mentioned above, this form of electronic delivery does not require the use of electronic signature.

The future solution of the Point of Single Contact can follow these processes, depending on European developments.


\textsuperscript{372} See http://www.mokk.hu/index.php?menuid=55

\textsuperscript{373} https://vny.nive.hu/statisztika/index.php?page=page1
15.3 Delivering electronic documents to service providers in the context of the
Point of Single Contact

15.3.1 The back-office – communication between the Point of Single Contact (PSC)
and the competent public administrations or private organisations

The identification of the relevant public administrations (ministries, organizations with national or local
responsibility) and the private or social organizations for the installation of the Point of Single Contact
should be provided by the feasibility study on the transposition of the Services Directive.

The tasks of CESPS about the back-office of the competent authorities was described above. It is
noteworthy that the usage of the Office Gate and the BEDSZ is required for the provision of the
necessary means for the communication between the public administration and the Client Gate and
BEDSZ for private persons or organizations. The system could accomplish all task of the future Point
of Single Contact, if the legal conditions allow them.

BEDSZ applies secured XML. There is a development project for the definition of SOAP architecture
for the Hungarian public administration in the same time.

15.3.2 The front-office – communication between the Point of Single Contact (PSC)
and the service provider

The legal framework is under reshaping for the simplification of administration and for other
requirements of the Services Directive as was mentioned previously.

The services of CESPS may be suitable for the electronic communication between the PSC and the
service provider. One of the services for the electronic processes is the “notification storage”. Each
natural person (i.e. a representative of the service provider) is allowed to access her/his Client Gate
on the Government Portal and access her/his own “notification storage”374, a secured storage space.

Here, the user may download a copy of the documents sent to the authorities and can store the
response documents of authorities on a safe storage area, either temporarily or permanently. The
user may ask documents from the authorities to be sent via traditional mail to her official address of
residence, to her/his e-mail address registered in the Client Gate in an encrypted or open e-mail, or as
an encrypted or open electronic document from the CESPS. The client may upload her/his public
encryption key to the key storage area, and upon request the authority encrypts the documents before
sending it.

374 http://www.magyarorszag.hu/allampolgar/szolgaltatasok/tarhely
For the uploading of documents or keys, only a suitable browser program is needed; however the installation of Java 2 Runtime Environment is recommended for the use of all CESPS functions.

The physical and organizational framework of the PSCs may be built on the experience of the 274 Document Bureaus and the lawyers’ offices involved in the registration of business associations.

15.4 Assessment – Plans, progress and proposals for further harmonisation

15.4.1 Current plans and progress in the implementation of the Services Directive

An advanced infrastructure has been built up for the electronic administration and the data transfer between the authorities in the Hungarian public administration. The client contacts are carried out electronically by the CESPS on the Governmental Portal. The Document Bureaus of the district centres are the physical contact points in most cases. The Central Document Bureau has an key role as a department of KEKKH. The mediatory role of the accredited lawyers’ offices between the businesses and the court of registry is an example for the public-private partnership in the implementation process of Services Directive. However, beyond the registry courts many tasks are performed by the Company Information Service as an organization of the Ministry of Justice and Law Enforcement.

The feasibility study currently being performed has to define which development direction shall be followed in the implementation process of Services Directive. It is necessary to take into consideration the new legislative requirements after the modifications, the consequences of the necessary simplification of the administration. Obviously the establishment of a central administrative organization is necessary between the many diverse affected institutions, particularly because of service providers applying from other Member States. For the same reason, the Hungarian structure of the Internal Market Information (IMI) system will need to be developed further.

The implementation of the Services Directive may be accomplished in the framework of the New Hungary Development Plan. One of the 6 priority areas of the New Hungary Development Plan is the tasks relating to state reform. Within the framework of the New Hungary Development Plan there are two relevant operational programs: the State Reform Operational Programme and the Electronic Administration Operational Programme.

As the main goal of the State Reform Operational Programme is to realize a change of culture in the operation of the public administration, the Electronic Administration Operational Programme focuses on establishing a new attitude towards the developments of the electronic public administration services. The new approach has two pillars: every project will be examined to determine how it serves

---

375 See e.g. Electronic Public Administration Operational Programme
the horizontal aims. The second pillar is the centralization of the horizontal services which can offer solutions for all systems (e.g. electronic payment), to avoid parallel developments.

The operational programs include the modernisation of the procedures, processes and services of public administration and the judiciary system with the use of info-communication technology, as well as the interventions aimed at the identification of the clients as a common element of all public services provided by info-communication devices. The programmes involve all sectors of public administration, but priority is to be given to the development of the central functions to be used in the form of services by all specialised systems.

In contrast to the State Reform Operational Programme, the Electronic Administration Operational Programme intends to achieve its objectives by supporting the deployment of electronic public administration.

The institution-oriented approach will be replaced by a service- and client oriented approach. The overall objective will be reached if the planned interventions of the Operational Programme satisfy the needs of the clients and the public administration. Meanwhile special attention should be paid to interoperability on European level.

The electronic “non-stop management of cases” continuously accessible from home to be established in the framework of the programme will enhance the effectiveness of the interventions of the operative programmes and the integrated implementation of the developments.

In terms of implementation of Services Directive there are some major players in the Hungarian public administration:

- The State Secretariat for ICT and e-Government (http://www.ekk.gov.hu/en) is responsible for creating the framework of conditions for the operation of the e-government, forming the main component of a service providing state, and for developing services for the electronic management of public administration.
- KOPINT-DATORG Info-communications Ltd is a company fully owned by the state http://www.kopdat.hu/angol/index_en.html. It is developing and operating the Governmental Portal, the CESPS and Client Gate, the Electronic Governmental Backbone etc.
- The Central Office for Administrative and Electronic Public Services (http://www.nyilvantarto.hu/kekkh/kozos/index.php?k=nyitolap_en&b=bal_eng), which operate and manage authentic state registers (e.g. personal data and address, crime, vehicle, private enterprises etc.), handle data processing and data supply from the registers for duly mandated parties, issue certain documents (e.g. identity card, passport, driving license etc.), develop the client-orientated administrative procedures and also improve the electronic public services.

On 20 November 2008, the Government adopted a draft bill about the amendment of Két and a new bill on the electronic public services, and introduced these to the Parliament. The new bill widens the functions of CESPS, of Governmental Portal, etc and establishes the Electronic Governmental Centre of Public Services. It should be operated by KOPINT-DATORG Info-communications Ltd. The new “case net” and e-mail address with “client store” for every user of the Client Gate would be implemented supporting the electronic communication between clients and authorities. The data of the
company register should be accessed by means of the new “case net”. Further services, including central archiving services, e-payment and call center can be installed when the bill is enacted by the Parliament.

The submission of applications will be significantly easier in the future. The authorities shall transform all paper forms with a general form designer program into electronic fill in form according to a government decree and the above mentioned bill as of 31 March 2009. Instead of downloadable forms to be printed and signed or electronic documents, all service providers will be able to use fill-out web forms designed on the same, general platform, which supports XML based data transfer and processing.

15.4.2 Suggestions for further European support initiatives

According to the experiences the implementation of both directives on the data protection and on the electronic signature, differences will arise to some extent in the Member States which will result in additional difficulties in the implementation of the Services Directive, causing problems for the service providers in other Member States. The use of the qualified electronic signature has not become common in electronic commerce; however, the identification or authentication of clients in electronic public services imposes heavier requirements than typically implemented in private businesses, justifying the use of such technologies.

However, without additional measures the interoperability of electronic signatures may not be assured in the applications of public administrations even at the national level. Projects initiated to solve these problems, planned earlier in the IDABC program, such as the European Bridge CA were not realized so far.

The creation of unified web forms, the implementation of the electronic identity cards, or improved electronic identity management on common platforms of the Member States may provide a lot of help. The lack of such measures will result in the incomplete and delayed implementation of the Services Directive.
16 Iceland

16.1 General framework for electronic documents in eGovernment applications

16.1.1 Electronic documents in eGovernment applications

There is no general framework for the use of electronic documents in Iceland, but in the Administrative Procedures Act no 37/1993 there is a general framework for processing matters electronically, included in Articles 35-40. The relevant articles regulate the authorisation for processing matters electronically, form requirements, originals and copies, electronic signatures, electronic procedure and preserving electronic material.

Article 36 in the Act handles form requirements and states: “When established law, custom or general administrative provisions require that material for a government authority or the parties to an issue be in written form, material in electronic form shall be considered to fulfil this requirement, provided that it is technically accessible to the recipient, allowing her/him to peruse its contents, save it and later transmit it.”

Article 38 in the act handles Electronic Signatures and states: “When established law, custom or general administrative provisions require material from a party or government authority to be signed, the authority may determine that electronic signatures can serve in place of handwritten signatures, insofar as electronic signatures assure, in a similar degree to handwritten signatures, the personal confirmation of the one from whom the material originates. A qualified electronic signature, as defined by the Act on electronic signatures, shall always be considered to fulfil the legal requirements on signatures.

When established law, custom or general administrative provisions require material or certain aspects of it to be certified, this requirement shall be considered to be fulfilled through certification by an electronic signature that conforms with the first paragraph above and confirms the aspects for which certification is demanded.

When established law, custom or general administrative provisions do not require material from a party or government authority to be signed, the authority may determine that it is permissible to use means other than electronic signatures in order to confirm electronic material.”

There are currently no specific technical requirements on electronic forms in government applications, but there is some work ongoing related to this, most notably e.g. efforts attempting to standardize electronic forms (through XML Schemas). There are also some measures in the new policy for the

---

376 See Annex I, Administrative Procedures Act no 37/1993
information society 2008-2012\textsuperscript{377} related to this, e.g. a measure on standardization and coordination in eGovernment. This measure includes among other issues selection of standards for government documents.

16.1.2 Electronic documents for the purposes of the implementation of the Services Directive

There are currently no plans yet on how to accept electronic documents from other countries. No legal or specific technical requirements have been defined but it has been decided that the Point of Single Contact (PSC) will be part of the National Portal, Island.is.

16.2 Specific document types

16.2.1 Extracts from commercial registers (Register of enterprises)

It is possible to view some basic information from the register of enterprises on the Internal Revenue Directorate (IRD) website\textsuperscript{378}. This is normal http on an open web. Certain commercial companies\textsuperscript{379} have concluded contracts with the IRD to access the register with the purpose of selling more detailed access to it. The document format that is used when this information is provided by these commercial undertakings is PDF. There is currently no use of electronic signatures (the PDF documents are provided in an unsigned format), but there are plans to change this in the future; however, no details have been announced yet. Thus, no specific measures are available right now to verify the authenticity of the documents. In the law on the register of enterprises\textsuperscript{380} there is an article on access to the register but it is very general. There is also an ordinance\textsuperscript{381} that states what should be included in a certificate from the register.

16.2.2 Criminal records

Currently electronic documents are not available from criminal records; only paper extracts are available.

Certificates from the police registry is one of the measures in the new policy for the information society 2008-2012, planned to start 2009. No further outlines or plans have been made at this time.

\textsuperscript{377} \url{http://eng.forsaetisraduneyti.is/media/utgefidefni/Iceland_the_eNation.pdf}
\textsuperscript{378} \url{http://www.rsk.is/fyrirtaekjaskra}
\textsuperscript{379} \url{http://www.creditinfo.is/}
\textsuperscript{380} \url{http://www.althingi.is/lagas/135a/2003017.html}
\textsuperscript{381} \url{http://www.reglugerd.is/interpro/dkm/WebGuard.nsf/key2/162-2006}
16.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations, orders or stakeholder bodies. While it is difficult to obtain a complete overview, it does not appear that the extracts issued by such private organisations are commonly issued in an electronic form. The legal possibility to do so exists, due to the implementation of the Signatures Directive, but in practice only paper documents are commonly issued. In instances where electronic documents are made available to the members of a specific profession, this is typically only done in the form of paper copies, notably PDF scans of the original documents.

Currently, no plans exist to make the use of electronic extracts mandatory.

16.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form. Thus, the only electronic certificates of insurance that are encountered in practice are unsigned scanned documents (typically in pdf or tiff formats), which are occasionally used in cases where originals are not required.

Currently, no plans exist to make the use of electronic certificates of insurance mandatory.

16.2.5 Proofs of qualifications

Generally only paper originals are available. While electronic copies might occasionally be presented in the form of unsigned scans, this is merely a matter of convenience. No specific rules or framework exist for electronic proofs of qualification and no plans have been proposed to mandate their uptake. Proofs of qualifications are both issued by private organizations and governmental.

16.2.6 Statements from the service provider

There are plans on standardised electronic forms which will be available at the PSC. It has not yet been decided how the service provider will deliver his electronic statements to the Point(s) of Single Contact, but it will probably be solved by a special webform with a possibility to upload attachments.
16.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

It has not yet been decided how public administrations or private organisations will communicate through the Point of Single Contact.

16.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

It has not yet been decided how public administrations or private organisations will send back to the service provider replies and documents through the Point of Single Contact (i.e. the ‘back office’ of the Point of Single Contact). The Ministry of Commerce is currently collecting the required information to identify all relevant administrations and organisations that have to be linked to the Point of Single Contact. Based on the outcome of this process, further decisions will be taken.

16.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

It has not yet been decided how public administrations or private organisations will deliver documents (e.g. permits to provide services) back to the service provider. Planning of this is in preparation.

16.4 Assessment – Plans, progress and proposals for further harmonisation

16.4.1 Current plans and progress in the implementation of the Services Directive

As stated before there are measures in the Policy for the Information Society 2008-2012 on e.g. standardization in eGovernment and introducing eIDs in communications with public bodies. The results of this projects will be implemented in solutions to be created for the Service Directive. Iceland would welcome an agreement on a common document formats and standardisation on eSignatures.
Appendix I
This appendix includes chapter 9 in the Administrative procedures act. (A draft translation)

Administrative Procedures Act
No. 37/1993, passed on 30 April 1993
With subsequent amendments (through October 2007)

CHAPTER IX
Electronic processing of government administration matters

Article 35 - Authorization for processing matters electronically

A government authority shall decide whether to offer the option of using electronic data communications for conducting a matter. From the outset of the matter, it must be easy for the party to find the requirements that her/his hardware and software must fulfill in order to carry out the matter electronically, with the government authority calling attention to these requirements according to circumstances. Such requirements shall be designed to allow for as many people as possible to be able to use the equipment they have. A government authority that has decided to utilize the authorization provided for in the first paragraph above shall communicate information electronically while handling a matter if a party to it has specifically requested this. The same applies when someone has on her/his own initiative used the electronic equipment for communicating with a government authority which was advertised on the authority's website as allowed for such communications.

A government authority may decide what requirements the material it will accept electronically must fulfill. Among other things, the government authority may stipulate that the material it accepts be presented on a special electronic form. In that case, standardised instructions must be provided on filling out the form and on the requirements set by the government authority.

Article 36 - Form requirements

When established law, custom or general administrative provisions require that material for a government authority or the parties to an issue be in written form, material in electronic form shall be considered to fulfill this requirement, provided it is technicallly accessible to the recipient, allowing her/him to peruse its contents, save it and later transmit it.

Article 37 - Originals and copies

When established law, custom or general administrative provisions require a document to be an original, material in electronic form shall be considered to fulfill this requirement, if it can be ensured
that the material has not changed from the original version. However, this shall not apply to business letters or other letters that tie financial privileges to the holder of the letter.

When established law, custom or general administrative provisions require the presentation of material in more than one copy, material in electronic form shall be considered to fulfil this requirement.

**Article 38 - Electronic signatures**

When established law, custom or general administrative provisions require material from a party or government authority to be signed, the authority may determine that electronic signatures can serve in place of handwritten signatures, insofar as electronic signatures assure, in a similar degree to handwritten signatures, the personal confirmation of the one from whom the material originates. A qualified electronic signature, according to the Act on electronic signatures, shall always be considered to fulfil the legal requirements on signatures.

When established law, custom or general administrative provisions require material or certain aspects of it to be certified, this requirement shall be considered to be fulfilled through certification by an electronic signature that conforms with the first paragraph above and confirms the aspects for which certification is demanded.

When established law, custom or general administrative provisions do not require material from a party or government authority to be signed, the authority may determine that it is permissible to use means other than electronic signatures in order to confirm electronic material.

**Article 39 - Electronic procedure**

Administrative decisions and other material in electronic form shall be considered to have been presented to a party when that party has had the opportunity of noting their contents. Any party to the issue is responsible for her/his hardware and software fulfilling the demands that are placed on it, in accordance with the first paragraph of Article 35, and that are necessary for her/him to be able to note the contents of the administrative decision or other material which the government authority is sending her/him in electronic form.

Requests and other material shall be considered to have reached a government authority when that authority has had the opportunity of noting their contents. Insofar as possible, the government authority shall confirm on its own initiative that it has received the material.

When established law, custom or general administrative provisions require a government authority to present material to a party in a verifiable manner, this requirement shall be considered to be fulfilled by using electronic equipment which confirms that the material has reached that party.

**Article 40 - Preserving electronic material**

Governmental authorities shall preserve electronic material in such a way that it will later be possible to verify its contents and origin in an accessible manner.
17 Ireland

17.1 General framework for electronic documents in eGovernment applications

17.1.1 Electronic documents in eGovernment applications

The general legal framework for the issuing and presentation of documents to the administration is to be found in the Electronic Commerce Act 2000. Section 17 of the Act provides that where a person or public body is required or permitted to present or retain information in its original form, then the information may be presented or retained in electronic form. It is subject to a number of conditions however and these are set out in subsection 2. In the first place, originals can be produced or retained in electronic form only where there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form as an electronic communication. Also the information must be capable of being displayed in intelligible form and it must have been reasonable to expect, at the time the information was generated in its final form, that it would be readily accessible so as to be useable for subsequent reference. The most important conditions are those which relate to the obtaining of the consent of the person or body for whom the document is required or permitted to be retained, or to whom it is required or permitted to be produced. In the case of both public bodies and private sector bodies, the consent of the person or public body to whom the information is required or permitted to be presented or for whom it must be retained, must be obtained. A further requirement applies in respect of public bodies only: the public body's requirements concerning information technology and procedural matters must be met. Those requirements must, however, be made public and must be objective, transparent, proportionate and non-discriminatory.

Section 18 provides that electronic information can be used to meet a requirement to produce or retain information. The operation of this provision is also subject to a number of conditions. In the case of a document to be produced, the information must be capable of being displayed in intelligible form. In the case of a document to be retained, information can only be retained in electronic form where, at the time of the generation of the final electronic form of the document, it was reasonable to expect that the information contained in the electronic form of the document would be readily accessible so as to be useable for subsequent reference. The same conditions with regard to obtaining consent and the fulfillment of public bodies technological and procedural requirements apply in respect of the production and retention of information in electronic form as have been outlined in relation to section 17.

Section 12 provides that where a person or a public body is required or permitted to give information in writing then that requirement can be met by writing in electronic form. Again the operation of this section is subject to a range of conditions similar to those set out in sections 17 and 18, in particular that it was reasonable to expect, at the time the information was given, that it would be readily accessible to the person or public body to whom it was directed, for subsequent reference; that consent has been obtained; and that in the case of a public body, that the body's technological and procedural requirements have been met. A further condition not encountered in sections 17 and 18 is that a public body's requirement that a particular action be taken by way of verifying the receipt of the information be met. This condition is also subject to the proviso that such requirements have been
made public and are objective, transparent, proportionate and non-discriminatory. The scope of this provision is broad in that the definition of ‘giving’ information includes making an application, making or lodging a claim, making or lodging a return, making a request, making an unsworn declaration, lodging or issuing a certificate, making, varying or canceling an election, lodging an objection, giving a statement of reasons, recording and disseminating a court order, giving, sending or serving a notification.

Section 16 is concerned with ensuring that requirements to execute documents under seal can be met through electronic means. It provides that where a seal is required to be affixed to a document that requirement is taken to have been met if the document indicates that it is required to be under seal and it includes an advanced electronic signature, based on a qualified certificate, of the person or public body by whom it is required to be sealed. This provision is subject to the same requirements with regard to consent as have been set out in relation to section 17 above.

The Electronic Commerce Act contains a number of exceptions. Section 10 of the Act sets out a list of laws which are excluded from the operation of the Act. These include laws governing wills, trusts and powers of attorney. In addition, laws relating the handling of interests in real property are outside the scope of the Act. An important exception is contracts for the creation, acquisition or disposal of such interests. Contracts for the sale of property may therefore be concluded electronically but the deed of conveyance cannot be in electronic form. Further exclusions apply with respect to laws governing affidavits and declarations and to the rules, practices or procedures of a court or tribunal. In addition, section 11 of the Act specifies a number of laws, the operation of which must not be prejudiced by any provision of the Electronic Commerce Act. These are tax laws and laws relating to government imposed fees, fines and penalties, the Companies Act, 1990 (Uncertificated Securities) Regulations, 1996;382 the Criminal Evidence Act, 1992, or the Consumer Credit Act, 1995, and the European Communities (Unfair Terms in Consumer Contracts) Regulations, 1995.383 Thus, for example, consumer credit contracts cannot be concluded online.

Section 24 underlines the voluntary character of the Act’s provisions by stating that nothing in the Act shall be construed as requiring a person or public body to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form, or as prohibiting a person or public body engaging in an electronic transaction from establishing reasonable requirements about the manner in which the person or public body will accept electronic communications, electronic signatures or electronic forms of documents.

17.1.2 Electronic Signatures

While the Electronic Commerce Act does provide a legal framework for the use of electronic signatures in cases where their use is required or permitted, the Act does not itself require the use of electronic signatures in any context. As noted above, the Act includes as a condition for the electronic presentation of documents to a public body that the public body’s requirements concerning information technology and procedural matters must be met. Those requirements, which could include the use of an electronic signature, must, however, be made public and must be objective, transparent,

382 S.I. No. 68 of 1996.
proportionate and non-discriminatory. The eliding examples of eGovernment applications involving the use of electronic signatures are: the Revenue Commissioners ROS online service allowing for the online submission of tax returns involving the use of advanced electronic signature based on a certificate issued by the Revenue Commissioners; and the Companies Registration Office online system which allows for the online filing of annual returns which are signed by means of an electronic signature.

17.1.3 Technical Requirement and Soft Law

In the case of both the Revenue Commissioners and the Companies Office, the technical requirements are set out on their respective websites.

17.1.4 Electronic documents for the purposes of the implementation of the Services Directive

Legislation to transpose the Services Directive in Ireland is envisaged but is at an early stage of development. Thus, there is no fixed strategy yet for the use of electronic documents in this context.

17.2 Specific document types

17.2.1 Extracts from commercial registers

The two main commercial registers which operate in Ireland are the Register of Companies and the Register of Business Names. Both registers are controlled by Companies Registration Office (CRO). In broad terms, extracts in the form of electronic documents are not available from these Registers although, in certain circumstances, applications for registration can be made electronically and the Registers are available to search electronically, with certain information being made available for free.

385 See the Registration of Business Names Act, 1963.
386 See www.cro.ie
Company Registration

It is comparatively easy to form a company. All that is required is:

- a memorandum of association;\(^{387}\)
- articles of association;\(^{388}\)
- Form A1;\(^{389}\)
- Payment of relevant fee.

These documents must be lodged with the Registrar of Companies under one of three schemes for registration, including an electronic company registration scheme designed to facilitate speedy company registration (certificate of incorporation issued within 5 working days). This allows the presentation of the relevant documentation in disk form (CRODisk) and the relevant registration fee is deducted from the presenter’s deposit account with CRO. However, the CRODisk system also requires a paper application form to be filed, in addition to the electronic form because the paper form contains various signatures, including a statutory declaration of compliance, and the Electronic Commerce Act 2000 currently excludes statutory declarations from its scope.

The Register of Companies is available for searching electronically. Certain information is available for free while other information or documents require payment of a fee. For example, it is possible to purchase a copy of a certificate issued at the time of registration. Free duplicate certificates can be obtained via the website. These certificates are generally acceptable for public service use only. While a certificate of incorporation is issued in paper form and is not issued electronically, the need for such electronic documents is lessened by the available of an electronic database of registered companies which is publicly accessible and searchable online.

\(^{387}\) Must contain provisions dealing with certain matters e.g. the company’s name, objects, and whether the members’ liability is limited. The memorandum must be in accordance with the First Schedule of the Companies Act 1963.

\(^{388}\) This document sets out the rules under which a company will regulate its affairs. Model articles are provided in the First Schedule of the Companies Act 1963.

\(^{389}\) This standard form includes details of the company name, registered office, the company’s directors and secretary and it includes a statutory declaration that the requisite formalities for incorporating a company have been followed.
Registration of Business Names

Where the economic operator is doing business under a name or style which is not his or its real name, then that name must be separately registered under the Registration of Business Names Act, 1963. An application for registration can be processed online although once all the relevant details have been submitted electronically, the presenter must print-off a signature page which must be sent with any other documentation and the relevant fee to CRO. Again, the Business Name Certificate is issued in paper form and not electronically although the need for such electronic documents is lessened by the availability of an electronic database of registered business names which is publicly accessible and searchable online.

Additionally, it is worth noting that CRO is a participant in the BRITE Consortium, which aims to link European business registers, and hence eliminate the need for exchanging extracts.

17.2.2 Criminal records

Police certificates which contain information on an individual’s criminal record, or lack thereof, are issued by local Superintendents in charge of the District wherein applicants reside, or formerly resided, in the Republic of Ireland. It is not possible to apply online. Certificates are issued in paper form. The introduction of electronic applications for police certificates is not envisaged in the foreseeable future due to issues around establishing the identity of applicants. Similarly, the introduction of electronic issuing is not envisaged because of the fact that certificates must be physically signed by the superintendent. It is worth noting that police certificates are not generally required in the establishment of a business in Ireland and most police certificates are issued in relation to visa applications.

17.2.3 Extracts from professional registers

Architects

The system of registration of architects is currently in a state of transition as legislation (Part 3 of The Building Control Act 2007) has recently come into force (May 2008) which designates the Royal Institute of Architects of Ireland (RIAI) as the registration body for architects in Ireland and as the competent body in the State for the purposes of the Architects Directive. The registration system is not yet fully operational. Meanwhile the RIAI continues to operate its system of membership of the RIAI.

With regard to meeting the requirements of Art.8 of the Services Directive that procedures and formalities relating to access to and exercise of a service activity and may be completed by electronic means, the situation regarding both applications for membership/registration and the issuing by the RIAI of proof of membership/registration must be considered.

390 Business Register Interoperability Throughout Europe; see http://www.briteproject.net/
Applications for membership/registration

In terms of applications for membership the current position is that while the RIAI does not provide for electronic submission of documentation associated with gaining membership of that body, it does provide for the downloading of application forms. See http://www.riai.ie. In terms of implementing Article 8, it has been suggested that a distinction must be drawn between the arrangements for recognising qualifications from other Member States and the arrangements for the obtaining of membership/registration on the basis of Irish qualifications. It is envisaged that there will be little difficulty in implementing the acceptance of electronic documents in the former case and indeed preparations in that regard are underway both at Commission level, by means of the Internal Market Information system (IMI), and through the European Network of Architects Competent Authorities (ENACA). Difficulties are however envisaged in relation to the first registration processes for architects in Ireland. This is because of the need for the submission of original documentation such as academic transcripts and also because there are alternative routes to registration which require the submission of a wide variety of supportive documentation.

Issuing of proof of membership/registration

With regard to the issuing of proof of membership, the system currently in place is for the issuing of such documentation in paper form on RIAI letterhead. If requested by the RIAI member they are also scanned and e-mailed.

Engineers

Applications for membership

Applicants may submit an application for membership of Engineers Ireland, the professional body for engineers in Ireland online. However the online application is merely to send personal details. A “Verification of Qualification” form must then be downloaded and completed manually by the applicant and by the College or university at which he or she has studied and this must be returned to Engineers Ireland by post or fax. This online facility is also only suitable for people with a qualification accredited by any of the 3 international accords in place. For applicants from outside the countries in question, the online facility will tell them to contact the Membership Department where they will be directed to download the “Alternative Routes to Assessment” form. Engineers Ireland are currently assessing their electronic application system and changes to “a more user-friendly format” may be instituted in the coming year.

Issuing of proof of membership

A letter of Verification of Membership can be generated and sent via email to the member.
17.2.4 Certificates of insurance

To the best of our knowledge, certificates of insurance are not issued in an electronic form. While it would be legally possible to do so under the terms of the eCommerce Act, in practice there seems to be no demand for electronic certificates, and so far there are no applications or services that require them, either in the public or private sector. In practice, proof of insurance may be tendered and accepted in the form of unsigned scanned documents (typically in pdf or tiff formats).

17.2.5 Proof of qualifications

Generally, these documents are only issued in paper form. While electronic copies of transcripts might occasionally be sent to applicants as an attachment to an email, these are not generally acceptable because they lack formal authentication, for example in the form of an official stamp or signature. Plans to issue electronic proof of qualification, while envisaged, appears to be a long way off.

17.2.6 Statements from the service provider

Statements from service providers are not commonly used as part of the process of offering services in Ireland. Applications processes may however require the submission of a CV giving details of experience (e.g. applications for a travel agent/tour operator licence, applications for membership of the RIAI (Royal Institute of Architects)).

17.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

The National Profile Questionnaire states that the Services Directive requires that the service provider must be able to communicate exclusively with the Point of Single Contact if he so chooses, however, in our communications with representatives from the Department of Enterprise, Trade and Employment the use of the word 'exclusively' was queried. The Department representative stated that there has not been any discussion in the Expert Group on the Transposition of the Services Directive on the exclusivity of the Point of Single Contact with regard to communicating with a service provider. Indeed, in his view, there will be occasions when a competent authority will need to communicate with a service provider outside the context of the Point of Single Contact.
17.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

In relation to identifying all relevant administrations and organisations that have to be linked to the Point of Single Contact, the representative of the Department of Enterprise Trade and Employment noted that this was an onerous task, particularly in light of the fact that there is potentially an unlimited number of services that fall within the remit of the Directive. However, the Department has begun the task of identifying the main organisations that will be involved in a pilot Internal Market Information system (IMI) that will connect competent authorities in different Member States.

The Department has also sent out a questionnaire to over 300 organisations that may act as a competent authority. Replies to this questionnaire are due back now and these replies will impact on the development of the Point of Single Contact. Regular meetings are held with other Departments and with other Sections of this Department to ensure all aspects of the transposition of the Directive are being addressed. Other competent authorities and organisations will be identified during 2009 and linked to the Point of Single Contact as applicable.

It is envisaged that the Internal Market Unit in the Department of Enterprise, Trade and Employment will probably be responsible for the operation of the Point of Single Contact, at least in the initial period following the transposition of the Directive but this may change in the light of experience. The transposing legislation will provide the necessary flexibility to change this, if circumstances warrant it. Moreover, the responsibilities, liabilities and legal obligations of competent authorities and the Department will be set out in the legislation that transposes the Directive in Ireland.

No advanced/web-service oriented standards and communication protocols are currently envisaged.

In term of progress, the Department is currently in a consultation phase with regard to the Point of Single Contact and it is hoped to have a mock-up version of the Point of Single Contact by the first quarter of 2009.

17.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Following communications with the representative of the Department of Enterprise, Trade and Employment, any requirements for change in the legal framework will be set out in the transposing legislation. For example, at present, the Department does not envisage translating the content of the Point of Single Contact into other Community languages. Other matters, e.g. as regards liability, will also be addressed in the transposing legislation (see above).

In relation to specific technical requirements for the delivery process, the representative from the Department noted that Article 5 of the Services Directive requires Member States to simplify the procedures needed to access a service activity. Under the terms of this Article, the Department will
ask competent authorities and other relevant organisations to undertake a risk based analysis to identify those procedures that need signatures and identification formalities and only to transfer those procedures to the electronic field that can be justified after taking this Article into account. For those procedures that do require an electronic signature the Department will ask that competent authorities will accept the use of the minimum standard agreed at comitology. The Department supports the EU Commission’s view that Member States should agree on the minimum level of technology that they will accept in the form of e-signatures. It is understood, from various meetings of the Services Directive Expert Group, that Member States will not be required to handle this technology. The Department assumes that any decision reached about the minimum level of e-signatures technology will only apply to a Member State to the extent that its Points of Single Contact opt to handle that level of technology.

Implementation plans in this regard are currently under deliberation.

17.4 Assessment – Plans, progress and proposals for further harmonisation

17.4.1 Current plans and progress in the implementation of the Services Directive

See above. Traditionally a light touch approach has been adopted in terms of the regulation of service provision in Ireland. The provision of some services have only become subject to regulation in recent years. For example, architects have become subject to a system of registration only since mid 2008. Such regulation as exists is very much paper-based. This reflects, in part, the permissive nature of the eCommerce legislation whereby the use of electronic document is predicated upon consent of the relevant bodies. Plans on the transposition of the Services Directive appear to be at an early stage.

17.4.2 Suggestions for further European support initiatives

Concerns were expressed within the Department that some Member States may make access to their Point of Single Contact conditional on having some form of electronic identification card. This would put service providers from those Member States, such as Ireland, that do not use Public Key Infrastructure projects at a serious disadvantage in terms of using those Points of Single Contact.
18 Italy

18.1 General framework for electronic documents in eGovernment applications

18.1.1 Electronic documents in eGovernment applications

The Italian lawmaker enacted, since the early nineties, many Acts in the field of e-government in general and of electronic documents in particular, and it is worthy to mention, for instance, Article 15 of the Law no. 59/1997, which expressly recognized the legal relevance of the electronic document (‘documento informatico’ in Italian) and of its digital transmission. Another important source in the area is the Decree of the President of Republic (‘Decreto del Presidente della Repubblica’, thereinafter D.P.R.) no. 445/2000 regarding the administrative documents (both paper-based and electronic), but undoubtedly the source that deserves the most attention is the Legislative Decree (‘Decreto Legislativo’, thereinafter D.Lgs.) no. 82/2005 (Code of the digital administration, ‘Codice dell’amministrazione digitale’ in Italian, thereinafter the ‘Code’).

The Code contains an entire section dedicated to the electronic document. As regards the requirements that the electronic document must respect, Article 20(1) of the Code states that such a document is valid and relevant to the ends set by the Law, in other words it has, from the substantial point of view, the same effects as the traditional written documents provided that the technical rules set forth by Article 71 (see infra) are respected and, more precisely, that (i) the identification of the author and (ii) the integrity and non-modification of the document are assured. As regards the effects of the electronic document as evidence before a judge, pursuant to Article 21(1) the electronic document to which an electronic signature has been attached will be basically evaluated by the judge on a case by case basis as regards its probatory value, provided the presumption that the signatory of the electronic signature attached to the document is the author of such a document.

The main criterion to confer full validity to the electronic document is thus the presence of an electronic signature, to be more precise a qualified advanced electronic signature according to the European legal framework, i.e. either (i) a qualified electronic signature (‘firma elettronica qualificata’395) or (ii) a digital signature (‘firma digitale’396). The general provisions regarding the

393 D.Lgs. 7 March 2005, no. 82, G.U. no. 112 of 16 May 2005.
395 The qualified electronic signature is, pursuant to Article 1(1)(r) of the Code, “the electronic signature obtained through electronic proceedings that guarantee the unambiguous connection to the
electronic signature are provided by Articles 24-37 of the Code, which set forth the legal distinction between (i) not authenticated electronic signature and (ii) electronic signature authenticated by a notary or other public officer. To give an example of the practical relevance of this distinction: if a person buys an immovable property, the contract must be signed with an electronic signature authenticated by a notary; in practice this means that the contract must be signed before the notary who checks the identity of the signatory. As concerns the technical requirements of the electronic document, the abovementioned Article 71 of the Code states that these shall be specified by one or more Decrees of the Prime Minister (‘Decreto del Presidente del Consiglio dei Ministri’, thereafter DPCM).

The government thus enacted the DPCM of 13 January 2004\(^{397}\) concerning the “technical rules for the creation, transmission, conservation, copying, reproduction and validation (including time validation) of the electronic documents”. This DPCM basically sets technical rules regarding the creation, use and verification of electronic signatures and states that the provisions adopted at international level or enacted by the European Commission in this field must be respected. To be more precise, as regards the creation and verification of the electronic signature, the certification must be based on the algorithm RSA (Rivest-Shamir-Adleman) with keys long at least 1024 bit.

The basic legal principle set forth by the DPCM, then, is that the keys (two keys) for the creation and verification of the signature can be assigned only to one signatory, pursuant to Article 4(1); furthermore, the DPCM sets forth the division between certification keys (‘chiavi di certificazione’) and subscription keys (‘chiavi di sottoscrizione’) and provides that the former can be generated only by the entity which is responsible for the provision of the service, while the latter can be generated by the signatory or by the certification-service-provider (Article 6 (1) and (2)).

Further technical rules regarding the recognition and verification of the electronic document are set by the Decree no. 4/2005\(^{398}\) of the National Centre for ICT in the public administration (‘Centro Nazionale per l’Informatica nella Pubblica Amministrazione’, thereafter CNIPA\(^{399}\)), which specifies technical details aimed to implement the Code and the abovementioned DPCM. This decree is a very good example of the relevance of the so-called ‘soft law’ in the field of IT law in Italy, given the fact that the lawmaker (parliament and government) is not in the right position to be continuously updated as regards technological innovations. CNIPA is a technical institution by the Office of the Prime Minister and its decrees and regulations are not, strictly speaking, sources of law but provide useful guidance and set technical requirements. Two provisions are particularly relevant: (i) Article 3 of the Decree person who made the signature and its unambiguous electronic attestation, created with means on which the person who made the signature can keep exclusive control and linked to the relevant data so that it is possible to check whether the data have been modified, and based on a qualified certificate and implemented through a safe item for the creation of the signature, such as the electronic items used for the creation of the electronic signature.”

\(^{396}\) The digital signature is, pursuant to Article 1(1)(s) of the Code, “a particular kind of qualified electronic signature based on a system of cryptographic keys, one public and one secret, linked to each other, that allow the signatory (through the secret key) and the recipient (through the public key) to disclose and verify the provenience and integrity of an electronic document or of a group of electronic documents.”

\(^{397}\) G.U. no. 98 of 27 April 2004.


\(^{399}\) See http://www.cnipa.gov.it
states that the profile of the certificates, in principle, shall be consistent with the specification RFC 3280, chapter 4, and with the specification ETSI TS 101 862 V1.3.2; (ii) Article 12 states that the cryptographic envelope that contains the electronic document basically shall be consistent with the specification RFC 2315, that it shall be of the type signedData and that for its codification the formats ASN.1-DER or BASE64 can be used.

In addition, it should be noted that the Italian Government takes part in a number of European projects, including Peppol and Stork, in connection with e-identity, e-procurement, and e-documents. Through Unioncamere the Italian delegation is also a part of Spocs (the ‘Simple procedures on-line for cross-border services’ pilot), focused on creating interoperability in the context of the Services Directive, managed by France and European Commission.

18.1.2 Electronic documents for the purposes of the implementation of the Services Directive

The Services Directive has not been implemented yet (November 2008) into national law (see infra at the end of paragraph for further details), nevertheless its transposition will necessarily reflect some basic principles listed in the Code. First, pursuant to Article 2(1), the central government and the local authorities shall guarantee the “availability, management, access, transmission, retention and usability of information in digital form”. Secondly, and specifically, Article 3 sets forth the principle that “the citizens and the enterprises have the right to ask and obtain the use of IT technologies in the communications with the central public authorities and with the suppliers of public services of the central government...”

Article 4 of the Code is equally pivotal, as it states (§ 1) that citizens and businesses have the right to participate in the administrative proceedings and have access to administrative documents though ICT technologies. With this regard, other relevant sources are Articles 59 and 60 of the D.P.R. 445/2000; the latter in particular provides for the interconnection of the existing networks of the public authorities in order to create a unique network of the public administration, provided that every authority shall individually set the technical and organisational criteria regarding the access to the documents and information in the light of the principles specified by the CNIPA.

Article 4(2) of the Code then states that every document “can be transmitted to the public authorities through the use of ICT technologies if it is created and sent with the respect of the applicable legal provisions.” The exploitation of ICT involves the use of certified e-mail (Article 6) and, from a different perspective, the possibility to make e-payments to the public authorities (Article 5). Provided this framework, it is interesting to analyse how the adoption of ICT technologies by the Italian public administrations (and therefore the implementation of the Services Directive) shall be carried on.

Given the complexity of the Italian public administration and the coexistence of (basically) national, regional, provincial and municipal authorities, every authority is independent when adopting ICT technologies and moving towards more updated modalities of working and communicating with citizens and enterprises. Pursuant to Article 12 of the Code, in fact, “the public authorities when organising their activities independently shall adopt ICT technologies”, and the central government has the task to promote the implementation and the use of networks as an instrument of communication between public authorities, citizens and enterprises (§ 4). More specifically, according to Article 16, the competences to set guidelines and stimulate, inter alia, the adoption of electronic
documents by public authorities is of the Office of the Prime Minister, of the Minister for Public Administration and Innovation and of the Minister for the Normative Simplification. The latter, in particular, has the duty to coordinate the initiatives linked to the simplification of the normative rules regarding the administrative proceedings, including the implementation of Chapter II of the Services Directive400. As it will be shown infra, then, the implementation of the Point of Single Contact follows a different path and the autonomy of the different public institutions involved will be partially compressed in favour of a unique solution at national level.

As regards the acceptance of electronic documents coming from Italy and other Member States, the principles described above apply, and therefore Article 20 and following of the Code will play a pivotal role. Such provisions do not specify whether or not the electronic document from service providers of other Member States, provided that all the abovementioned requisites are met (namely the presence of a qualified advanced electronic signature), can be accepted by Italian public authorities. It is nevertheless possible to give a positive reply to this question, at least from the general legal point of view, taking into account the provision of Article 21(4) of the Code. As mentioned above (see supra for further details) this Article sets rules regarding the value as evidence (i.e. the probatory value) of the electronic document, and § 4 says that such rules apply also if the electronic signature is based on a certificate issued by a certification-service-provider not established in a Member States provided that some conditions are met401.

In other words, from this provision we can infer that Italian electronic signatures and electronic signatures from another Member State (e.g. electronic signatures based on a certificate issued by a certification-service-provider established in another Member State) have the same legal value and that, as a basic principle, the electronic documents signed with it shall be accepted by public authorities. The opposite conclusion would create a discrimination against electronic signatures from other Member States and this discrimination may be considered, prima facie, not to be fully consistent with the principles of EC.

From the practical point of view, nevertheless, it is pivotal to consider that the Italian legislation, namely the Code, requires that the electronic document must be signed with a qualified electronic signature (‘firma elettronica qualificata’) or a digital signature (‘firma digitale’) and therefore the requisites may be higher than in other Member States. Provided that actually there is not yet full interoperability between the different electronic signature standards adopted in Europe, the Italian public authorities accept electronic documents coming from other Member States if the standards used there, mainly as regards the electronic signature, are the same as the Italian ones. At the same time, the Italian government would support a European system of mutual recognition of electronic signatures coming from other Member States.

For what concerns the setting up of specific legal and technical requirements as regards document types and formats, signatures, etc, this is definitely a work in progress, and the Italian government is participating in European projects in this field, promoting the adoption of ETSI standards.

401 Basically the same conditions set forth by Article 7(1) of the Electronic Signature Directive.
Finally, some notes about the transposition of the Services Directive into national law. From the legal point of view, such transposition will be made with a D.Lgs. enacted by the government under assignment conferred by the Parliament with the so-called Community Act (which is the main instrument for implementing community legislation, and governs the timing and the manner of transposing community directives). This D.Lgs. has already been drafted by the government and it was originally planned to be enacted at the end of 2008, but the political crisis and the elections held in the first semester of 2008 had the consequence to postpone the enactment of the D.Lgs. to spring/summer 2009. From a different perspective, the main problem linked to the implementation of the Services Directive in Italy is the screening of the existing national and regional legislation and administrative regulations. Most of the provisions of the Services Directive, in fact, concern topics of regional competence, and the Regions are actually analysing how to implement these rules and evaluating which parts of their legislations and administrative regulations must be reformed. The entire process should be completed by the end of 2008.

The Italian presentation of the portal’s prototype took place on 20 November 2008 during the so-called “Jamboree” organized jointly by the Dutch delegation and the European Commission.

### 18.2 Specific document types

#### 18.2.1 Extracts from commercial registers

Commercial registers have been affected heavily by the adoption of IT technologies by Italian public authorities. Without entering into further details, we just mention Article 31 of the Law 340/2000 regarding the delivery of applications and documents in electronic format to the offices competent for the commercial registers (i.e. the Chambers of Commerce) and the Decree of the Ministry for Economic Development of 2 November 2007 which implements the electronic form for opening a new business. For what concerns the delivery of electronic certificates and documents by the offices competent for the commercial registers, the applicable source is the Decree of the Ministry for Economic Development of 15 February 2008 which (i) regulates the modalities of request and delivery through electronic means of the electronic certificates and (ii) sets technical specifications as regards the structure and format of the electronic certificates. The electronic extract from the commercial register, to be more precise the certificate of inscription in the commercial register, can be acquired through an offline or an online application and it will be delivered by the competent authority online, i.e. in the form of an electronic certificate. The extract will mention the following elements: (i) name of the Chamber of Commerce that delivered the extract; (ii) the kind of certificate (with this

---

402 The Government prepared a document that should help and guide the national and regional authorities when screening the existing legislation that can impede the free provision of services. The document (‘Guida per il Monitoraggio relative alla Direttiva “Servizi””) is available online: [www.politichecomunitarie.it/file_download/418](http://www.politichecomunitarie.it/file_download/418) (last accessed: 13 November 2008).


regard the Decree of the Ministry for Economic Development of 25 February 2005 mentions explicitly the certificate of inscription in the commercial register; (iii) the statement that the certificate is delivered only in electronic format; (iv) the data regarding the person/company that required the document; (v) the name and address of the recipient; (vi) the statement regarding the use of the certificate; (vii) the date of delivery.

The extract shall be a non-modifiable file in PDF/A format with the electronic signature of the office competent for the commercial registers. For what concerns the standards of the electronic signature, the technical requirements and specifications provided by the abovementioned CNIPA Decree no. 4/2005 apply (see therefore above for further details). Furthermore, the Italian Chambers of Commerce provide an online service for registered users (usually lawyers, accountants, notaries, etc) that can have access to most of the economic data of a company (e.g. balance sheets, bankruptcy proceedings, etc) through the following website: http://www.registroimprese.it/dama/comc/navcom?cl=IT.

18.2.2 Criminal records

As regards criminal records (official statements of past convictions and pending criminal proceedings, in Italian ‘certificato penale’ and ‘certificato dei carichi pendenti’), they are issued by the Office of the Prosecutor by any Italian Court in paper format. The applicable source is the Decree of the Ministry of Justice of 25 January 2007 which sets technical and procedural rules to implement the D.P.R. 313/2002 (Consolidated Text of the criminal records). This Decree instituted a central electronic database of criminal records for the whole country in order to facilitate the exchange of information between the public administrations concerned. The institution of a centralised database undoubtedly allows to avoid many ‘gaps’ related to the transmission of notices of criminal convictions between competent offices. In other terms, traditionally the criminal records were not accurate and updated and the implementation of the electronic database could render the information more precise.

More specifically, Article 26(1-4) of the Decree sets forth the principle that every citizen can request a copy of his criminal records to every competent office (i.e. the Office of the Prosecutor) in Italy. The record will then be issued to the applicant or to another person authorised by the applicant and the public officer that delivers the record shall control the identity of the applicant (in case the other person authorised by the applicant will collect the record, he shall submit a copy of the identity card of the applicant). This means that it is still not possible to obtain criminal records in electronic format. On the other side, the applicant shall be allowed to send the request to the competent office by filling in an online form, as specified by Article 26(6) of the Decree: some Offices of the Prosecutor already allow online requests, like for instance in Milan (see http://www.procura.milano.giustizia.it/casellario/richiesteonline.php).

---

18.2.3 Extracts from professional registers

It is difficult to provide an exhaustive overview of the state of the art as regards professional registers, due to the plurality of professional organisations and the fact that they are dispersed all around the country. In practice, only paper-based certificates and extracts are given, and often the professional organisations accept only paper-based applications and requests. As far as the author is aware, there are no plans or projects to implement electronic-based delivery of extracts of professional registers, at least at national level, but for further details see infra under point D.
18.2.4 Certificates of insurance

Certificates of insurance are generally issued only in paper-based format, given the fact that there seems to be no demand for the electronic version from the public and private sector and that in some cases it is necessary to have (and to show) the original certificate printed on special paper aimed to assure that the certificate is not fake. This applies for instance to insurance for cars and trucks, whose certificate of insurance shall be posted on the windscreen and cannot be removed.

18.2.5 Proofs of qualifications

The same considerations made above as regards certificates of insurance apply to proofs of qualifications, so that in general terms electronic proofs of qualifications are the exception rather than the rule. It is extremely difficult to provide a complete overview of the situation in the whole country, provided that such certificates are usually issued by private or public organisations dispersed in Italy and no common or general rules apply. As regards, for instance, proofs of academic qualifications, some Universities allow students and former students to view online and print their qualifications\(^{409}\), although often such certificates are not legally valid unless they are printed and validated by a public officer and/or a tax stamp is stuck on the certificate.

18.2.6 Statements from the service provider

As regards the statements from the service provider, being a private entity he is free, as a general rule, to issue electronic statements, but what is more relevant is to see whether or not public authorities accept such electronic statements. We saw above that quite often Italian public offices allow the submission of requests and applications online and, from a different perspective, often original certificates can be substituted by a self-declaration or a self-statement made by the applicant, usually through a predefined paper-based or online form. With this regard however there is not yet a general framework that applies to all public authorities and solutions are rather adopted on a sector by sector basis.

\(^{409}\) See for instance the service provided by the University of Padua (http://www.unipd.it/sis/index.html).
18.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

18.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

The first example of Points of Single Contact, in Italian ‘sportelli unici per le attività produttive’, has been defined originally by the D.P.R. no. 447/1998\(^\text{410}\), which established points of single contact at local level with the aim to simplify the proceedings to obtain licenses for the building, enlargement, renovation and reconversion of productive establishments, for the execution of works inside the establishments and the individuation of the areas designated to productive establishments. Article 1 of the Code, then, states that this ‘sportello unico’ shall be made available to the citizens and enterprises in IT-format (i.e. a website) and that all documents, applications, etc can be sent in electronic format.

The Point of Single Contact defined by Article 8 of the Services Directive is nevertheless more complete than the one defined by the D.P.R. of 1998 and service providers should be allowed to make “all procedures and formalities relating to access to a service activity” through it, therefore it has to communicate with a wider plurality of public administrations and private organizations. With this regard the Italian competent authorities, namely the Ministry for Economic Development, the Minister for Public Administration and Innovation, the Italian league of Chambers of Commerce (Unioncamere) and CNIPA, are planning the implementation of a web portal/Point of Single Contact for service providers. The prototype of the portal, whose address will most probably be http://www.impresa.gov.it/, has been presented to the European Commission last 14 October 2008.

Contrary to the abovementioned ‘sportelli unici’, which are established at local level, the Point of Single Contact/web portal will be national and therefore a uniform delivery solution at the national level will be adopted. The core of the portal will be centered on the services provided by the Chambers of Commerce, with many links to other institutions and organizations that are necessary or useful for the service providers. With this regard, special attention is dedicated to the professional organizations (e.g. lawyers, architects, engineers, etc) that must give necessary authorizations to the service providers or that keep lists of service providers active in a certain province/town, thus a consistent part of the work of the Point of Single Contact will be to communicate with these many organizations.

For the reasons explained above, i.e. that the core of the services available through the portal are those provided by the Chambers of Commerce, the management and implementation of the Point of Single Contact will be shifted from the Ministry for Economic Development to Unioncamere, under the supervision of CNIPA.

From the legal point of view, then, the implementation of the Point of Single Contact will not require any change in the current framework regarding liabilities, responsibilities, etc and the existing rules and practices will be applicable. This because, as envisaged by the Ministry for Economic Development...
Development and the Minister for Public Administration and Innovation, the main mission of the portal is to gather together already existing ‘elements’, i.e. IT-based services already available for service providers, with of course new features like the links with professional organizations. From the technical point of view no advanced/web-service oriented standards are planned to be used, in order to keep the system as easy and user-friendly as possible.

Finally it is interesting that the current status of implementation of the Point of Single Contact is very advanced and that all national public authorities concerned are ready to operate the portal.

18.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

The Point of Single Contact will have, apart from the function of accepting documents, requests, etc of the service providers for the public administrations and private organizations concerned (see above), the task to deliver documents, licenses etc from the public administrations/private organizations to the service providers.

For the Point of Single Contact/portal to operate, the existing provisions stated in the Code and in all other sources, starting from the Acts and regulations in the field of administrative law (mainly Law no. 241/1990) are sufficient and fully applicable to the new IT-oriented solutions, and therefore, as pointed out above, the government does not plan to enact any reform. As regards the language of the Point of Single Contact, the portal will be in Italian and the public administrations/private organizations will issue documents in Italian. At the same time, the certificates and documents that the service provider submits through the portal shall be translated in Italian (if, of course, the original version is in another language), although the English version of the portal is currently under development.

For what concerns the technical requirements for the delivery process, the competent authorities do not plan to develop new standards, protocols, etc and the existing solutions will be adopted. The Italian authorities, in fact, and especially CNIPA, made a lot of effort in the period 2001-2006 to set formats for electronic documents, rules on electronic signature etc and therefore all these resources will be fully exploited with the implementation of the Services Directive.

In conclusion, as specified above, the current status of implementation is very advanced, also as regards the front-office side.

---

18.4 Assessment – Plans, progress and proposals for further harmonisation

18.4.1 Current plans and progress in the implementation of the Services Directive

Italy made great advancements in the last years in the field of e-government with the aim to render the public administration (traditionally perceived as ‘heavy’, slow and rather inefficient) modern and efficient. The ultimate goal is to reduce red tape for citizens and companies and create enablers, rather than barriers, for them. An important issue to highlight regarding the implementation of the Services Directive, in particular the Point of Single Contact, is that public authorities, mainly at the level of the central government, strongly collaborate with other institutions, like the league of the Chambers of Commerce, that deal every day with service providers. In other words, the Italian approach seems to be bottom-up and top-down at the same time. For further considerations, see infra.

One of the main issues that come out from the analysis carried out in the previous pages is related to the differences that are still existing among Member States in the field of electronic signature. It has been confirmed by the Officer who validated the information contained in this report, in fact, that the Italian legislation, namely the Code, requires that electronic documents are signed with a qualified advanced electronic signature, and the standards adopted in other European countries do not seem to be always fully consistent with the Italian ones. This can be a big barrier to the full implementation of the Services Directive and will limit the acceptance rate of electronic documents coming from other Member States by the Italian public authorities and private organizations in charge of conferring authorizations or licenses to the service providers.

Therefore it would be suitable to set up a mechanism of mutual recognition of electronic signatures (and thus electronic documents) at European level, based on trust between national authorities of the Member States. This could be a first step to set common rules and standards for all Member States with the aim to abolish inconsistencies and technical differences between the standards and typologies of electronic signatures adopted by the European Countries. At the end, as in many other fields, the alternatives are the mutual recognition of existing differences or the harmonization of rules, standards, proceedings, etc.

Another relevant point, in which European initiatives would be useful, concerns the language barrier. We saw that the Point of Single Contact/portal in Italy will operate in Italian and probably in English, but this does not mean, as said above, that the documents sent by the service providers to the Point of Single Contact and then to the administrations and organizations concerned can be in their original language. It is of course true that it is impossible to require public officers to speak all European languages, and that the costs for the translations cannot be fully borne by the Point of Single Contact or by the administrations and organizations concerned. At the same time, it would be advisable that Member States recognize the existing situation de facto, i.e. that English is the most used business language in the world. In other words, it would be feasible that the Point of Single Contact accepts electronic documents written at least in English, in order to reduce the costs for the service providers and increase the level of European integration. It would thus be necessary to generalize already existing good practices. To give a concrete example, it is possible to obtain a birth certificate in English issued by the municipality of Rome, or a proof of academic qualification in English delivered
by Dutch Universities; but often these documents must be translated in the (or one of the) official national or regional language(s) in order to be accepted by the public authorities or private organizations in charge of the proceedings. As regards Italy, and more in general at European level, the implementation of the Services Directive could be the right moment to remove this inconsistency.

18.4.2 Suggestions for further European support initiatives

We saw above that the implementation of the Point of Single Contact follows a top-down and a bottom-up approach at the same time. It is undoubtedly true that the involvement of the league of Chambers of Commerce is a key aspect for the successful operation of the Point of Single Contact, but this is not enough. The government is aware of the fact that the participation of the professional organizations is pivotal, and it is advisable that these organizations, or at least the most important ones in terms of representativeness, are involved in the creation and implementation of the portal (i.e. the Point of Single Contact). Two aspects have to be taken into account: firstly, that this consideration applies also to the other European countries; secondly, that such an involvement cannot be limited to professional organizations but should be extended obviously to local and regional authorities.

It has been pointed out above, in fact, that many requirements and issues of the Services Directive are the competence of regional authorities in Italy, and therefore it seems advisable that they are involved (and in fact a meeting of the central government and the Regional authorities in the permanent group State-Regions – ‘Conferenza Stato Regioni’\(^{412}\) – has already been planned) in order to avoid inconsistencies. In other words, the risk is that the service providers established in some Regions can benefit from the Point of Single Contact more than those located in other Regions. Yet, this point concerns not only Italy, but also other Member States.

\(^{412}\) See http://www.statoregioni.it/ (last accessed: 14 November 2008).
19 Latvia

19.1 General framework for electronic documents in eGovernment applications

19.1.1 Electronic documents in eGovernment applications

At the national level, Latvia does not have a generic framework related to electronic documents in eGovernment applications in general. While a several eGovernment applications are available to the public, they are regulated and implemented on an ad hoc basis.

Generally, Latvian applications do not rely on electronic documents as such, either in the form of files that need to be presented by the end user to the application; or in the form of files that are issued to the end user after the conclusion of a transaction. Rather, the Latvian approach to eGovernment revolves largely around web services and around establishing trusted relationships between public administrations and selected private sector organisations for the direct exchange of authentic information. Thus, when information needs to be exchanged, typically this will be done through these trusted networks rather than by requiring the creation of a specific electronic document.

Thus, as regards electronic documents, no generic legal framework or technical requirements exist, as electronic documents are not currently in common use in public administrations.

According to the Latvian eGovernment conception413 eGovernment is defined as an access to provision of public services and realization of the state administration that is based on the use of IT possibilities and operation principles typical for eCommerce by ensuring improvement of quality and efficiency of public services and increase of participation of the general public in the state administration.

In order to coordinate activities necessary for the modernization of the state administration in 2004 a position of a minister for special assignments for electronic government affairs (the “Minister”) was created. The Minister is responsible for eGovernment, information society and information technologies policy development, implementation and coordination.

For the practical implementation of strategically significant activities in the information society development and eGovernment field in Latvia set forth by the Cabinet of Ministers, the Secretariat of the Special Assignments Minister for Electronic Government Affairs (the “Secretariat”) – the state

administration institution under the direct supervision of the above-mentioned Minister – was created in 2005\textsuperscript{414}.

Political support to the Minister and the Secretariat is ensured by the Information Society National Council, a consultative and coordinating institution chaired by the Prime Minister of Latvia. Another consultative institution is eGovernment Coordination Council of Latvia, which promotes carrying out of the eGovernment projects.

In September 2005 the Cabinet of Ministers adopted the eGovernment Development Program for years 2005 – 2009\textsuperscript{415}, which sets forth the main tasks in the sphere of eGovernment, responsible authorities, involved authorities, necessary financing and time frames for implementation of the above-mentioned tasks. The eGovernment Development Program is closely linked with initiatives eEurope 2005 Action Plan and the new European level strategy “2010 – A European Information Society for growth and employment” adopted by the European Commission on 1 June, 2005.

The basic action lines of the eGovernment Development Program are to improve state and municipal information technology infrastructure and collaboration between state registers, to create new channels for government services, to create new e-services for citizens and business, to create new state information systems and to develop municipality's information systems.

European Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures was transposed into Latvian law through Electronic Documents Law effective as of 1 January 2003\textsuperscript{416}. Its latest amendments regarding qualified certificates and trusted certification service providers effective as of 7 July 2006 were adopted due to introduction of a qualified eSignature in September 2006.

For implementation of the Electronic Documents Law Regulations of the Cabinet of Ministers No. 473 on order of elaboration, formatting, storage and circulation of electronic documents in state and municipal institutions and order of circulation of electronic documents among state and municipal institutions and natural and legal persons were adopted on 28 June 2005\textsuperscript{417}.

The purpose of the Electronic Documents Law is to provide a precise regulatory framework for the use of electronic documents and electronic signatures.

\textsuperscript{414} Web site in English available at http://www.eps.gov.lv/index.php?&93
\textsuperscript{416} In Latvian – Elektronisko dokumentu likums, available in Latvian at http://pro.nais.dati.lv/naiser/textc.cfm?Key=0103012002103132806&Lang=03
\textsuperscript{417} In Latvian - Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām, available in Latvian at http://likumi.lv/doc.php?id=111613&from=off
Definitions of an electronic signature and a qualified electronic signature in the Latvian Electronic Documents Law correspond to their definitions in the Directive. The Latvian Electronic Documents Law defines a so-called secure electronic signature in the same way as the advanced electronic signature in the Directive, and additionally regulates a qualified electronic signature.

Since September 2006 all state and municipal institutions are obliged to accept electronic documents signed with a qualified electronic signature. However, electronic signatures are not widely used by state institutions and private parties.

The ‘eSignature’ officially arrived in Latvia on 4 October 2006 when Latvia Post started to issue their certified eSignature cards. The new cards can be used to sign documents electronically and access a variety of on-line eServices. In accordance with the Electronic Documents Law all state and municipal institutions must accept documents signed using eSignature cards. In practice, however, only a very limited number of electronic documents are submitted to state or municipal institutions.

Electronic document is defined in the law as any data which is created, stored, sent or received electronically, which ensures the possibility of utilising such data for the performance of some activity, realisation of a right and protection.

The Secretariat offers assistance when a public institution cannot properly deal with a document signed by eSignature. Theoretically it is possible to submit documents signed by the eSignature to all public institutions. Nevertheless, due to lack of any practice for use of electronic documents a person might be reluctant to use electronic documents. For example, it is not clear how the electronic document would be handled in the court institutions or whether at all these documents would be accepted in the same manner as paper documents.

Thus communication by means of electronic documents is regulated in Latvia, however, it is not widely used. The eGovernment applications rely more on web-based solutions.

19.1.2 Electronic documents for the purposes of the implementation of the Services Directive

In Latvia, the creation of a "Government Portal" was one of the first phases of eGovernment development. The project was initiated in order to provide possibilities for an easier and faster access to information of state institutions. Currently, the Government portal has a number of references to the public administration institutions where the users of this portal can obtain relevant information as regards electronic public services.

The development of information systems was carried out separately in each institution and municipality. Typically this development was carried out with assistance of foreign investments. Thereafter, several information systems have been developed for each respective administrative

418 The site can be reached by the address: www.latvija.lv;
body. Mostly these are different systems. The functionality of each system depends on what kind of services the public institution offers. As a result of this uncoordinated development there is no centralized development of information systems.

All existing eGovernment systems are developed by the system administrators themselves. Usually these systems are made for satisfying needs of a particular administrator. Some of these institutions offer online services on their web site.

In accordance with the conception on creating a single point of access (the "Conception") the Government portal will be used to provide information to the providers of services. Currently this portal is the single place where a person may receive inter-institutional services. Authorized access is possible via secure eSignature or using authorization via an online banking account. Payment can be made via online banking solutions offered by almost all banks. This portal currently offers the user access to several eServices. All of these services can be used to request certain documents.

Several problems have been identified in the Conception that will require a solution to be fully developed for the Point of Single Access, namely:

- Circulation of information between different state institutions is not very effective. In ca. 30% of cases when a person submits a document to the state authorities he or she must attach information issued by another institution;
- IT solutions for administrative procedures vary from one institution to another. Therefore it is not currently possible to create a unified information system.
- Each institution supports its own IT infrastructure. Therefore, it would be necessary to optimize IT solutions to increase effectiveness.
- Various institutions use different methods of identifying the applicants.

Therefore full implementation of the Services Directive will require extensive work, to first of all, centralize the institutions and, secondly, to provide their services via eGovernment applications.

The implementation of the Services Directive is expected to be done in phases in Latvia.

The Government Portal will be extended to include more information in relation to economically active entities.

For Latvian service providers, the approach is likely to focus on using the eSignature capabilities. For service providers of other Member States, Latvian administrations are currently examining how they can incorporate trusted lists of CSPs into their solutions. With regard to signature level requirements, while the Latvian eSignature is considered to be a qualified signature, it has not yet been decided whether this will also be required of electronic signatures in the cross border context. Before making

this decision, Latvian administrations first wish to see the direction in which European initiatives are evolving to determine how they can easily integrate an optimal number of e-signatures from other Member States. Nevertheless, current eSignature solutions can be adjusted for use in cross border transactions.

Regarding the document types to be supported, Latvia is similarly awaiting European developments. Generally speaking, as noted above, Latvian administrations do not require the use of electronic documents from the end users, and thus a large margin of flexibility still remains in making implementation choices. If interoperability would require the uptake of a specific standard, it would likely be possible to integrate this, provided that the standard is sufficiently supported at the international level.

From a practical perspective, service providers wishing to become economically active in Latvia using electronic means only will need to contact the Government Portal that will function as a Point of Single Contact. Providing the needed information will initially be limited to relatively low-tech and accessible means, such as on-line web forms for data entry. As mentioned above, it is not yet clear which document types and signature requirements will be imposed; this depends to a large extent on the evolutions at the European level in the next few months. After that, the Point of Single Contact will be responsible for ensuring the proper follow-up, including by interacting with any competent administrations or private organisations. The processes to be followed in order to do so will of course depend on the requirements of the specific service provider\textsuperscript{420}.

19.2 Specific document types

19.2.1 Extracts from commercial registers

In the Latvian legal system the Company Register manages several different registers (to name most important of the Commercial Register, Commercial Pledge Register, Insolvency register and others). All of these registers are accessible online using services of a private company Lursoft IT SIA.

Functionality of the Company Register applications may be divided into two modules.

First, a private Latvian company Lursoft IT SIA holds an electronic database of the Company Register (Lursoft electronic database web site – \texttt{www.lursoft.lv}). Thus, information registered with the Company Register is accessible to any interested party electronically after a conclusion of an agreement for specific services with SIA Lursoft IT regarding the access to all or specific types of information registered with the Company Register, obtaining a username, ID and password for login to the database on the Lursoft web site and payment for the respective services. Please note however that

\textsuperscript{420} Telephone conference with Ms. Inese Betaka, Head of International Policy Unit, Minister for Electronic Government Affairs on 03.12.2008
this database is not considered as official (although in practice it is very widely used and considered precise).

Second, the Company register itself provides various information on its services on its website www.ur.gov.lv. In addition, all types of application forms that have to be submitted to the Company Register according to Latvian law can be downloaded from the website and filled in electronically. Nevertheless, they can be submitted to the Company Register only in paper format. Paper attestations are made available instead of electronic solutions.

19.2.2 Criminal records

A criminal records certificate can be obtained from the Information Centre under the Ministry of the Interior of the Republic of Latvia (in Latvian: Iekšlietu ministrijas informācijas centrs) provided that a written (paper) application is submitted by the applicant.

The Ministry of the Interior of the Republic of Latvia (in Latvian: Iekšlietu ministrijas informācijas centrs) has launched an on-line service for the delivery of criminal record certificates in Latvia. At present only natural persons may order criminal records certificate electronically using the electronic criminal record certificate order system. In order to request criminal records certificate electronically, the user must hold online banking account (currently only clients of Swedbank are accepted). The electronic certificate can be requested through a web portal (see e.g. http://www.ic.iem.gov.lv/?q=lv/node/316) by filling in the electronic application form. Provided that the electronic application is filled in and the fee paid on-line, a (paper) criminal records certificate can be issued within few business days. The requested certificate can be directly picked up from the Ministry of Interior or delivered to the applicant by registered mail.421

19.2.3 Extracts from professional registers

Certificates issued by the relevant professional registers would be delivered in a paper format. It is questionable whether electronic versions of such certificates can be considered authentic. Several registers are available online to check whether person has actually received certain certificate; however, these are usable for information purposes only.

19.2.4 Certificates of insurance

With regards to travel, real estate (house or flat) or car insurance, it is possible to buy an insurance policy online provided that the electronic insurance contract is paid through the e-banking system or

credit card. The insurance policy will then be sent to the applicant via email. However, these are unsigned documents (typically in Word or PDF format).

19.2.5 Proofs of qualifications

Proofs of qualifications are usually delivered in a paper format only.

19.2.6 Statements from the service provider

Statements made by the service provider himself will likely be integrated into the Government Portal as web forms to be completed and signed. It is not yet clear which requirements will be imposed on such statements, beyond the comments made above: in all likelihood, a limited number of signature solutions will be supported in cases where signatures will be required, and it is not unlikely that further implementation efforts will require some other solutions.

However, this is not a certainty yet, as it depends to some extent on European and national developments in the near future.

At this point in time there a is fully integrated tax declaration reporting service, electronic tax declaration system (EDS)\(^{422}\), through which individuals and legal entities are able to submit tax related reports via Internet and/or e-mail. The EDS ensures the complete electronic interaction between the user and the public service provider. The user of the system may submit all documents electronically as well as complete all the formalities on-line and receive electronic service consecutively. Electronic tax reports are registered with the State Revenue Service under (in Latvian: Valsts iejēmumu dienests). The system is available to both Latvian nationals and non-nationals.

It has to be noted that the system does not use secure eSignature at the moment. The verification of a person is confirmed on a conclusion of electronic agreement with the State Revenue Service for the provision of electronic tax reporting services. The user name and password for EDS is sent to the user by e-mail after the conclusion of electronic agreement. This data enables to identify a person who is allowed to submit the tax declaration form electronically. A similar system could also be used for a Latvian Point of Single Contact.

\(^{422}\) In Latvian: Elektroniskā Edelkarēšanas Sistēma; official webpage available at: http://deklaravimas.vmi.lt/PublicPages.aspx?ID=1&file=0
19.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

19.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

In accordance with the Conception there are three possible models envisaged for situations when the service provider wants to gather necessary information. The first interaction model is based on situation when service provider searches for information. In this case he can conduct the search in the Government portal www.latvija.lv and receive links to respective state institution, application form and translations of regulations.

The second interaction model will be applied to the case when service provider needs additional help from Latvian institutions. In that case he can communicate using the same portal and the answer will be provided by the respective state institution. The Investment and Development Agency of Latvia (in Latvian: Latvijas Investīciju un attīstības aģentūra) will be the institution responsible for addressing the questions to the respective institutions. This agency will also deal with questions that are not related to the subject of Services Directive. Also the distribution of questions can be done automatically through a ticketing system; in this case the respective institution will receive it, answer it and mark as done.

The third and final model is fully automated interaction between service provider and portal. This will be achieved by developing automated solutions to typical cases.

Except for the first model which is partially offered already, all necessary infrastructures are still under development to achieve the full functionality desired of the PSC.

19.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

As was mentioned above, the function of the eGovernment web portal is to ensure the provision of public services by electronic means. The portal administers the communication with the client (recipient of the service) and a control function i.e. identify the client, accept the client’s request to perform the service, direct it to the responsible institution and deliver the final results to the client. The public institution which provides services, on the other hand, performs the service requested and delivers the final result to the portal.

It has to be noted, that requirements in relation to the communication with the service provider has not been defined yet as a result of the early stage of the implementation process. However it is most likely that XML based solutions will be used in communication.
19.4 Assessment – Plans, progress and proposals for further harmonisation

19.4.1 Current plans and progress in the implementation of the Services Directive

The provisions of Services Directive must be implemented into Member States national laws by December 2009. The final results as regards the changes of the transposition of the Services Directive into Latvian law will be apparent only by the end of the implementation period.

The conception provides that a pilot project for the establishment of the point of single contact, has to be structured in the near future. However, as confirmed orally by the representative of the Secretariat423, the establishment process of the procedures in relation to the point of single contact is at an early stage and for that reason the information currently available is limited.

As confirmed by the representative of the Secretariat424, the Latvian government approved that the Investment and Development Agency of Latvia will function as a formal point of single contact for the purposes of the Services Directive. In accordance with the verbal information provided by the Ministry of Economy, the formation of this contact centre is still ongoing. The setting-up of the necessary legal framework as regards the procedure and functioning of such a contact centre will be the main priority of the responsible institutions in the immediate future. Only one contact centre will be established as a PSC, namely the Investment and Development Agency of Latvia, and its presence will be virtual as well as physical.

In the light of the foregoing, it could be concluded that in Latvia the process of implementation of the Services Directive is in very early stages. Presently, it is not possible to evaluate what national implementing measures are to be adopted with a view of transposing the directive.

19.4.2 Suggestions for further European support initiatives

The main prospect is the full implementation of the Services Directive into Latvian legal system under which all types of administrative procedures could be performed electronically. At present there is a decentralized and distorted system as regards the electronic procedures in eGovernment applications in Latvia. This has as a result that some institutions take their own approach concerning the creation of information exchange systems which enable online data exchange. As it was mentioned above, there is an initiative to develop a fully functioning point of single contact which would help public

423 Telephone conference with Ms. Inese Betaka, Head of International Policy Unit, Minister for Electronic Government Affairs on 03.12.2008
424 Telephone conference with Ms. Inese Betaka, Head of International Policy Unit, Minister for Electronic Government Affairs on 03.12.2008
administration institutions and officials to co-operate more effectively through electronic means. Therefore, it is expected that the point of single contact would not only facilitate the exchange of authentic information among public authorities and service providers, but also will harmonize the cross-border interoperable eGovernment services.
20 Liechtenstein

20.1 General framework for electronic documents in eGovernment applications

20.1.1 Electronic documents in eGovernment applications

Liechtenstein does not have a generic framework related to electronic documents in eGovernment applications in general.

There is currently no legal framework in place that determines the technical and procedural requirements that electronic documents need to meet.

Our portal services still rely on submitting forms in the same way as applies in the "paper world" at the front desk of our public authorities. The number and variety of eGovernment services cannot be increased significantly because personal identification currently cannot be obtained electronically. Our eID will be launched in April 2009 allowing the creation of eGovernment services with personal identification and signing possibilities.

Our parliament adopted the IT- and eGovernment strategy 2008 – 2011. Applications will be rapidly created based on reusable basic services and systems using an eGovernment architecture adopting the principles of the European Interoperability Framework. Launching an eID implies supporting applications for an extended usage of eGovernment services, and the same applies to fulfil the requirements of the Services Directives.

Various projects have been defined and will be launched within the given time frame to reach the goals of our eGovernment strategy. Our eForms application already signs the acceptance of submitted forms and soon will allow a reusable integration and safe usage of personal documents within the workflow of eGovernment services using a so called eSafe. Required permit prolongations, as an example, will be announced electronically, together with required additional user interactions.

Requesting an official authenticated document using an eGovernment service should allow a postal delivery and/or the creation of an eDocument, stored in a personalized safe place for further usage. The definition of formal and technical requirements for an interoperable usage is essential. This is on our side not yet defined for local usage and the requirements for European wide interoperable usage possibly will be provided in near future.
20.1.2 Electronic documents for the purposes of the implementation of the Services Directive

Within the context of the Services Directive the same approach to electronic documents will be followed as on a local usage. The service provider should be able to deliver documents electronically but the verification process will be difficult. National registers allow partial verification for local citizens. The usage of IMI will allow some verification but documents from private sectors, as professional organisations, possibly can only be verified at the place of origin. The acceptance of scanned and self signed documents in relation to presented paper documents at the front desk, which equally are difficult to be verified, needs further discussion and agreement. This is true also on the local national level, possible acceptance and requirements are not yet defined.

The implementation of the Services Directive is expected to be done in phases in Liechtenstein. So far efforts have mostly focused on finalising the required screening exercises, in which a very strong emphasis has been placed on following the Directive’s requirements for administrative simplification in a strict manner, thus avoiding the need for original documents whenever possible, to minimise problems related to this issue.

Our approach will be focusing on a limited number of currently most frequently used cross-border services, implementing them on a local level, always keeping in mind the specialities to be observed for a cross-border usage by service providers fulfilling the Services Directive’s requirements.

The creation of a national signature verification platform must be followed by a European wide signature verification platform, using national CSP trusted lists and an agreed minimal level of signature standards usage, ensuring reliable cross border information exchange.

By the end of 2009 a limited set of services using eID identification will be available locally and accordingly on a European level. The role of eDocuments will evolve locally and correspondently on an international level through the existence of applications that create, accept and process eDocuments.

Web services will play a key role for authorisation to ensure interaction with official registers on a local and European level.

Regarding the document types to be supported, Liechtenstein is similarly awaiting what trends are emerging at the national level in other Member States.
20.2 Specific document types

20.2.1 Extracts from commercial registers

As noted above, electronic documents are not yet used by the Liechtenstein Public Administration. Thus no information is available about technical characteristics, document format and electronic signatures used.

Consequently there is no special legal framework in place for this type of document and no statement is possible about document validity determination.

Within near future extracts from commercial registers, as from other registers, can be obtained electronically. This implies the existence of adopted eDocument technical definitions and the specific legal framework in place.

Signing of eDocuments by the competent authority will be accomplished using specific basic services, allowing an equal signature creation process and an overall usage by eGovernment services. As stated in a recent eCertificates study “In summary, there is no framework yet for eProcurement or electronic certificates and attestations in Liechtenstein”

http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/ecertificates_country_en.pdf

20.2.2 Criminal records

Extracts from the penal register exist in Liechtenstein, but only in a paper format.

The statements made for extracts from commercial register apply accordingly to criminal records.

20.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations. Extracts issued by such private organisations are commonly issued in paper form. Beside the paper form typically PDF scans of the original documents are used and submitted electronically by e-mail.

The statements made for extracts from commercial register apply accordingly to document types issued by private organizations.
20.2.4 Certificates of insurance

This is another document type issued by private organizations and the same statements as in respect of extracts from professional registers apply to this document type.

20.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications.

20.2.6 Statements from the service provider

Statements made by the service provider himself will likely be integrated into our eGovernment portal as web forms to be completed and signed. It is not yet clear which requirements will be imposed on such statements and how to integrate, an interoperable signature solution will be needed, a European wide challenge.

20.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

20.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

The identification of the competent public administrations and private organisations and the interaction with them will be implemented through the usage of services within the new eGovernment infrastructure. As part of that infrastructure a technical application platform will be used to design and build the needed services and applications in respect of communication between public administrations, private organisations and the service provider.

The role of the Point of Single Contact we mainly see as monitoring the delivery of services, interacting on demand with the competent public administrations or private organisations.
20.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Replies and documents that have to be delivered to the service provider will be available for the service provider interacting with the eGovernment portal as defined within the workflows of these eGovernment services on a local national usage, adapted to the requirements of the service directive in terms of translated information and other aspects.

The delivery of documents from public administrations or private organisations back to the service provider subsequently will be also integrated into the respective workflow. Secure and reliable interaction with the IT-systems of private organisations by means of loosely coupled system technologies could be accomplished in the near future.

The communication path used behind that “black box”, mainly with human interaction using existing and established communication channels, won’t be visible to the service provider but must provide disruption free execution. To which extent signed eDocuments will emerge in Europe and be commonly used will have also an impact on the design of our mainly “virtual” Point of Single Contact.

eGovernment services must be provided on a national basis first together with the launch of our eID, always keeping in mind a future interoperable European wide usage.

20.4 Assessment – Plans, progress and proposals for further harmonisation

20.4.1 Current plans and progress in the implementation of the Services Directive

As mentioned in the overview above, Liechtenstein cannot yet rely on an advanced infrastructure in place that can be adapted for the implementation of the Services Directive.

Specifically with regard to electronic documents, Liechtenstein’s experience can be disregarded, as there is no usage in the private and public sector yet, mainly through the lack of certificate usage. This hopefully will change rapidly after the launch of our eID.

20.4.2 Suggestions for further European support initiatives

Liechtenstein’s plans regarding electronic documents and delivery are not yet defined. As in the “paper world” at the front desk we possibly will give the requesting party in the world of “eGovernment” the option to choose postal delivery and on request additionally an electronic, signed copy, a kind of eDocument that can be place in a personal eTreasure for future use.
As on the national level we need the possibility to verify electronic signed documents on a European level. This implies the usage of agreed minimal standards in the process of creating eSignatures to allow subsequently also the building of means for the verification process. Trusted lists of national QCSP together with agreed minimal required signing standards are helpful to reach the goals not only of the Service Directive but also to progress towards an extensive information exchange within Europe.

Authentication is a major issue within national eGovernment and thus also on a European level. The ongoing initiatives on eIDM must be strengthen to finally allow Pan European eGovernment Services access and interaction with national IT-systems.
21 Lithuania

21.1 General framework for electronic documents in eGovernment applications

21.1.1 Electronic documents in eGovernment applications

The general framework as regards electronic documents in eGovernment applications in the Republic of Lithuania is the Specification Requirements for Electronic Document signed with the eSignature approved by the Order of the Director General of Lithuanian Archives Department under the Government of the Republic of Lithuania as of 9 October 2008, No.V-119 (the “Specification Requirements”). These specifications establish the main requirements as regards the use of electronic documents signed with the eSignature by public administration institutions, government and municipality institutions and other public organizations.

Please note that the specification requirements as regards the use of electronic documents by non-governmental organizations, natural and legal persons are only recommendatory. Furthermore, the specification requirements for electronic documents envisage the requirements as regards the contents of electronic documents, the requirements for the metadata of electronic documents and the requirements as regards the use of eSignature of electronic documents.

The Rules of Management of Electronic Documents (the Rules), approved by the Order of the Director of the Lithuanian Archives Department under the Government of the Republic of Lithuania No V-12 as of 11 January 2006, establish the procedure for preparation, management, record, storage, and destruction of electronic documents as well as set functional requirements for the Management systems of electronic documents, and are obligatory for the institutions of public administration. In addition, the Rules define the notion of an electronic document. An “electronic document” as established in the Rules is a document, prepared or received using information technology devices, provided it bears a legally valid electronic signature and the document is recorded with the Management system of electronic documents.

The Recommendations on adaptation of internal rules and working regulations of public institutions for the purposes of introducing eSignature and electronic documents (the “Recommendations”) were adopted by the Information Society Development Committee under the Government of the Republic of Lithuania as of 7 December 2006, No. T-152. The purpose of these Recommendations was to


426 In Lithuanian: Elektroninių dokumentų valdymo taisyklės, Nr. V-12, 2006.

427 In Lithuanian: Dėl rekomendacijų įstaigų darbo reglamentų, vidaus darbo tvarkų keitimui ir organizavimui diegiant elektroninį parašą, pereinant prie elektroninių dokumentų naudojimo patvirtinimo, Nr. T-152, 2006.
harmonize and regulate the different approaches used among the public institutions in order to facilitate the use of eSignatures in public administration.

The Recommendations concerning contents of the electronic document, contents of the signed electronic document and the use of the format of the electronic document by the state institutions and organisations when exchanging official electronic documents by electronic means approved by the Order of the Director of the Information Society Development Committee under the Government of Republic of Lithuania as of 7 December 2006, No. T-153 were prepared in order to ensure the compatibility of the exchange of electronic documents among the state institutions and organizations. The Recommendations lay down the specifications as regards the format of electronic documents as well as the electronic signature requirements for electronic documents when state institutions exchange electronic documents among themselves.

The Law on the Amendment of Article 19 of the Law on Public Administration No X-239 as of 9 June 2005 sets out the framework for the exchange of electronic documents between the state and municipal institutions and the public and the use of electronic signature. It provides that the requests submitted by citizens through electronic means must be signed using an electronic signature. In turn, the answers of state institutions shall be signed with an advanced eSignature by the head of the Public Administration institution concerned, or a person authorized by him.

As regards the Electronic Signature, it has to be noted that in Lithuania the Directive 1999/93/EC (the Electronic signatures directive) has been implemented by the means of the Law on Electronic Signatures (the Law on eSignatures), which regulates the creation, verification and validity of electronic signatures, signature users’ rights and obligations, establishes the certification services and requirements for their providers, as well as the rights and functions of the institution of electronic signature supervision.

The Law on eSignatures establishes that an electronic signature is any data, which are inserted, attached to or logically associated with other data for the purpose of confirming the authenticity of the latter and (or) identification of the signatory. It has to be noted that the definition of electronic signature thus corresponds with the provisions of the Electronic signatures directive. Therefore, the Law on eSignatures provides for all possible forms of electronic data authentication and identification of the signatory. Furthermore, the Law on eSignatures also defines the “secure electronic signature”, corresponding to the notion of an advanced electronic signatures in the Directive.

---

428 In Lithuanian: Rekomendacijos dėl elektroninio dokumento turinio, pasirašyto elektroninio dokumento turinio ir elektroninio dokumento formatų naudojimo valstybės institucijoms ir įstaigoms elektorninėmis priemonėmis keičiantis oficialiais elektroniniais dokumentais, Nr.153, 2006.

429 In Lithuanian: Lietuvos Respublikos 2005 m. birželio 9 d. Viešojo administravimo įstatymo 19 straipsnio pakeitimo ir papildymo įstatymas, Nr. X-239.


431 Law on Electronic Signature, Article 2(4).
21.1.2 Electronic documents for the purposes of the implementation of the Services Directive

In Lithuania, the creation of a “Government Portal”\(^{432}\) was one of the first phases of eGovernment development transferring public services into the electronic environment. This project was implemented by the Information Society Development Committee under the Republic of Lithuania (in Lithuanian: \textit{Informacinės Visuomenės Plėtros Komitetas prie Lietuvos Respublikos Vyriausybės (IVPK)}).\(^{433}\) The project was initiated in order to unify all Lithuanian state institutions into one universal system of administration of official information, and by doing so, to provide possibilities for an easier and faster access to information-related activities of state institutions and start rendering services of public administration on the Internet. Currently, the Government portal has a number of references to the public administration institutions where the users of this portal can obtain relevant information as regards electronic public services.

The framework document of eGovernment services in Lithuania is the Position Paper on eGovernment, adopted by Decree No 2115 of the Government of the Republic of Lithuania as of 31 December 2002.\(^ {434}\) The main objectives envisaged in this paper are the improvements of the provision of public services by means of electronic communication.

The general framework as regards the exchange of electronic documents among the state and municipal institutions is foreseen in the law on the amendment of article 19 of the Law on Public Administration as mentioned above. In addition, an amendment to the law on the right to obtain information from state and municipal institutions, No X-383 as of 10 November 2005\(^ {435}\), stipulates that requests for information can be sent electronically only if it is possible to identify the requestor.\(^ {436}\) All written documents (including electronic documents) must be signed.\(^ {437}\) Furthermore, the documents of an institution which are electronically presented to the applicant are equal to written documents, provided that the security of the text is ensured, and it is possible to identify the signatory.\(^ {438}\)

The exchange of electronic documents in the public sector has been supported by the electronic signature infrastructure. With regard to the use of an eSignature, it has to be noted that the XAdES electronic signature format is required. The Specification Requirements provide that the electronic documents must be signed with secure electronic signature composed in accordance to the XAdES standards and in compliance with the W3C Recommendation “XML-Signature Syntax and Processing”.

---

\(^{432}\) The site can be reached by the address: www.epaslaugos.lt; www.govonline.lt; www.evaldžia.lt

\(^{433}\) Official webpage available at: http://www.ivpk.lt/main_en.php

\(^{434}\) In Lithuanian: Elektroninės Valdžios Koncepcija


\(^{436}\) Article 12 (2) of the Law no X-383.

\(^{437}\) Ibid, Article 12 (6).

\(^{438}\) Ibid, Article 17 (2).
As it is provided in the IVPK’s yearly report on the implementation of the law on eSignature, the major issue which raises certain problems is the technical compatibility as regards the formation of eSignature. This is because different eSignature and software formation and verification equipment is used in the market. For example, electronic document and eSignature created by one kind of software would be difficult to read by another kind of equipment even though the equipment would match the formally created standards. In order to solve this problem it is recommended to renew the standards base and to seek the compatibility of such standards among the Member States.

Another problem which raises concerns is the storage of electronic documents. Currently, the Lithuanian Archives Department under the Government of the Republic of Lithuania (in Lithuanian: Lietuvos Archyvų Departamentas) is not ready to accept electronic documents for keeping. In addition, the method and format as regards the transfer of electronic documents to the Archives Department, which would ensure secure storage of electronic documents, are not determined either. During the period of 2007-2011, the Archives Department intends to conclude the project for the establishment of the infrastructure and technical specifications as regards the storage of the authentic electronic documents in the state archives.

Moreover, in relation to electronic documents one has to mention the Information System for Lithuanian Membership of the European Union (LINESIS) project. This system helps to register, accumulate and distribute documents received from the European Union system U32Mail/Extranet. EU documents are received only in electronic format through the U32Mail special program and are automatically registered in LINESIS. The objective of this system is to coordinate the activities of Lithuanian institutions, in particular, to assure that the accepted acts of EU law are transferred into national law and put into practice without any barriers.

21.2 Specific document types

21.2.1 Extracts from commercial registers

The Centre of Registers of the Republic of Lithuania (in Lithuanian: Registru Centras, web portal: www.registrucentras.lt) operates the Certification Centre [RCSC], which provides certification and time stamping services. It provides certification services as regards signing of electronic documents, transmitted through the internet, with a qualified eSignature in order to safeguard the senders identity and guarantee the integrity of electronic document.

439 In Lithuanian: Elektroninio pašto priežiūros institucijos Lietuvos Respublikos elektroninio pašto įstatymo įgyvendinimo kasmetinė ataskaita; available at: http://epp.ivpk.lt/


441 http://www.registrucentras.lt/rcsc/
Extracts from the Register of Real Estate may be accessed online through the portal mentioned above. The Real Estate public electronic service (NETSVEP) was established in order to ease the work of the Centre of Registers and Notaries. This electronic service is provided to natural persons and legal entities which are registered users of the system. Firstly, it is required to present an application and conclude an agreement on the provision of data with the Centre of Registers. Then it provides the applicant with a password which enables to connect via Internet to the central data bank, view the information and print it out.

The Regulations of the Register of Real Estate approved by the Resolution No 1129 of the Government of the Republic of Lithuania as of 12 July 2002 lay down that extracts from the Register of Real Estate may be obtained through electronic means.442

Through the NETSVEP system, the Notaries are able to receive all the information concerning the real estate transactions through the electronic means and then send it directly to the Centre of Registers. The purpose of this project was to create a service which will operate as a “one shop window” in the real estate transactions. Using this system the information concerning real estate transactions is easily transferred through the electronic means to Notaries and other parties to the transaction. Notaries are able to transfer this information through the electronic means to the Centre of Registers.

Please note that it is planned to establish a service through which the Legal entities will be able to exchange the information and provide documents, financial reports in an electronic form to the Register of Legal Entities.

21.2.2 Criminal records

A criminal records certificate can be obtained from the IT and Communications Department under the Ministry of the Interior of the Republic of Lithuania (in Lithuanian: Informatikos ir Ryšių Departamentas prie Vidaus Reikalų Ministerijos) provided that a written application is submitted.

The Ministry of the Interior of the Republic of Lithuania (in Lithuanian: Vidaus Reikalų Ministerija) recently launched a new on-line service for the delivery of criminal record certificates in Lithuania. At present only natural persons may order a criminal records certificate electronically using the electronic criminal record certificate order system (ETPUS – Elektroninio Teistumo (Neteistumo) Pažymų Užsakymo Sistema). In order to request a criminal records certificate electronically, the user must hold an e-banking account. The electronic certificate can be requested through a web portal (see e.g. http://www.ird.lt/etpus/) by filling in the electronic application form. Provided that the electronic application is filled in and the fee paid on-line, a criminal records certificate can be issued within one

business day. The requested certificate can be picked up directly from the Ministry of Interior or delivered to the applicant by registered post in a paper format or sent via email. 443

21.2.3 Extracts from professional registers

Certificates issued by the relevant professional registers would normally be delivered in a paper format. It is questionable whether electronic versions of such certificates can be considered authentic.

21.2.4 Certificates of insurance

Since January 2008 the State Social Insurance Fund Board under the Ministry of Social Security and Labour (SODRA) offers e-Servicing System for the Insurers referred to as EDAS, which is a new possibility of cooperation between the insurers (people who are obliged to pay their state social insurance contributions) and SODRA. EDAS allows the insurers to submit the social insurance references and applications electronically, as well as to get information from the database electronically. 444

Using the new system, the insurers will be able to form and submit electronic reports on personal social insurance and present applications as documents having legal power.

Certificates can be ordered electronically, however, they are issued in paper format.

With regards to travel, real estate (house or flat) or car insurance, it is possible to buy the insurance policy online provided that the electronic insurance contract is paid through the e-banking system or credit card. The insurance policy will then be sent to the applicant via email.

21.2.5 Proofs of qualifications

Proofs of qualifications are documents issued by private and public sector for which only paper originals are available. It is questionable whether electronic versions of such certificates can be considered authentic.

21.2.6 Statements from the service provider

443 Ministry of the Interior of the Republic of Lithuania [in Lithuanian: Lietuvos Respublikos Vidaus Reikalų Ministerija]

444 See http://www.sodra.lt/index.php?cid=2881
Statements made by the service provider would most probably be incorporated into the websites of the relevant institution. For example, there is a fully integrated tax declaration reporting service, electronic tax declaration system (EDS)\textsuperscript{445}, through which individuals and legal entities are able to submit tax related reports via Internet and/or e-mail. The EDS ensures the complete electronic interaction between the user and the public service provider. The user of the system may submit all documents electronically and complete all the formalities on-line and receive electronic services consecutively. Electronic tax reports are registered with the State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania (in Lithuanian: \textit{Valstybinė Mokesčių Inspekcija prie Finansų Ministerijos}). The system is available both to Lithuanian nationals and non-nationals.

It has to be noted that the system does not use secure eSignatures at the moment. The verification of a person is confirmed on a conclusion of electronic agreement via on-line registration with the State Tax Inspectorate for the provision of electronic tax reporting services. The user name and password for EDS is sent to the user by e-mail after the conclusion of electronic agreement. This data enables to identify a person who is allowed to submit the tax declaration form electronically.

21.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

21.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

One of the obligations envisaged in the Services Directive is for the Member States to ensure that service providers will be able to complete all procedures and formalities through the "point of single contact" in order to simplify the access to and exercise of their service activities.

With regard to the Lithuanian strategy, no implementation details have been determined yet. However, it is foreseen that validation of information through the EU Internal Market Information System (IMI) will play a significant role for the exchange of information between public administrations and point of single contact.

21.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

As it was mentioned above, the function of the eGovernment web portal is to ensure the provision of public services by the electronic means. The portal administers the communication with the client (recipient of the service) and control functions i.e. identifies the client, accepts the client’s request to

\textsuperscript{445} In Lithuanian: \textit{Elektroninio Deklaravimo Sistema}; official webpage available at: \url{http://deklaravimas.vmi.lt/PublicPages.aspx?ID=1&file=0}
perform the service, directs it to the responsible institution and delivers the final results to the client. The public institution which provides services, on the other hand, performs the service requested and delivers the final result to the portal.

It has to be noted, that requirements in relation to the communication with the service provider has not been defined yet as a result of an early stage of the implementation process.

21.4 Assessment – Plans, progress and proposals for further harmonisation

21.4.1 Current plans and progress in the implementation of the Services Directive

The final results as regards the changes of the transposition of the Services Directive into Lithuanian law will be apparent only by the end of the implementation period.

The Services Policy Division within the Ministry of Economy of the Republic of Lithuania\textsuperscript{446} (In Lithuanian: Ūkio Ministerija\textsuperscript{447}) is responsible for coordination of transposition of the Services Directive into Lithuanian national law. The Decision of the Government of the Republic of Lithuania No. 1097 of 6 November 2006 “On adoption of the implementing measures for 2007-2010 of the strategy of development of public administration until 2010”\textsuperscript{447} (the Order on Implementing Strategy) lists a number of measures which have to be implemented by various responsible institutions. The implementing measures, as listed in the Order, are developed with a view of a step-by-step implementation of the Services Directive.

The Order on Implementing Strategy provides that a pilot project for the submission of information and completing the administrative procedures using means of electronic communications has to be structured by the end of 2008. However, as confirmed orally by the Ministry of Economy, the establishment process of the procedures in relation to the point of single contact is at an early stage and for that reason the information currently available is limited.

As confirmed by the officials of the Ministry of Economy, the Lithuanian government approved that the Lithuanian Development Agency (LDA)\textsuperscript{448} will function as a formal point of single contact for the purposes of the Services Directive. In accordance to the verbal information provided by the Ministry of Economy, the formation of this contact centre is still ongoing. The setting-up of the necessary legal framework as regards the procedure and functioning of such contact centre will be the major priority to

\textsuperscript{446} Official webpage available at: \url{http://www.ukmin.lt/en/}.

\textsuperscript{447} In Lithuanian: \textit{Dėl viešojo administravimo plėtros iki 2010 metų strategijos įgyvendinimo 2007–2010 metų priemonių plano patvirtinimo.} Available online in Lithuanian at: \url{http://www3.lrs.lt/cgi-bin/getfmt?C1=e&C2=308360}

\textsuperscript{448} In Lithuanian: \textit{Lietuvos Ekonominės Plėtros Agentūra (LEPA)}; official webpage available at: \url{http://www.lda.lt/en/index.html}
the responsible institutions in the immediate future. In accordance to the Services Directive, the precise concept of the point of single contact has already been decided i.e. only one contact centre will be established, namely LDA, and its presence will be virtual as well as physical.

The contact centre has to be established and fully operating as from 1 January 2010. In the light of the foregoing, it could be concluded that in Lithuania the process of implementation of the Services Directive is in very early stages. Presently, it is not possible to evaluate what national implementing measures are to be adopted with a view of transposing the directive.

21.4.2 Suggestions for further European support initiatives

The main prospect is the full implementation of the Services Directive into Lithuanian legal system under which all types of administrative procedures could be performed electronically. At present there is a decentralized and distorted system as regards the electronic procedures in eGovernment applications in Lithuania. This has as a result that some institutions take their own approach concerning the creation of information exchange systems which enable online data exchange. As it was mentioned above, there is an initiative to develop the fully functioning point of single contact which would help public administration institutions and officials to co-operate more effectively through the electronic means. Therefore, it is expected that the point of single contact would not only facilitate the exchange of authentic information among public authorities and service providers, but also will harmonize the cross-border interoperable eGovernment services.

In relation to the electronic ID cards, it has been announced by the Ministry of the Interior on 4 December 2008 that Lithuanian citizens will be able to use a new type of electronic ID card which will allow to identify the person in the electronic environment as well as to sign electronic documents. This will be implemented as from 1 January 2009. The electronic ID cards will be used as an eSignature and will guarantee effective exchange of electronic documents between service providers and users of the eGovernment services.
22 Luxembourg

22.1 General framework for electronic documents in eGovernment applications

22.1.1 Electronic documents in eGovernment applications

Luxembourg has not yet enacted a legal framework that specifically determines the requirements that documents issued or presented to the administration need to meet.

However, on the one hand, Luxembourg has implemented the Directive 1999/93/EC on a Community framework for electronic signatures. On the other hand, as a practical point, Luxembourg has planned out the technical requirements for certain online administrative procedures or formalities, such as those accessible to individuals but not relating to the access to a Service and those accessible to entrepreneurs relating to the VAT declarations.

- Legal framework of the electronic signatures

Implementing the Directive 1999/93/EC on electronic signatures, the Luxembourg law of 14 August 2000 relating to the ecommerce, as amended, defines the electronic signature as a set of data, inseparable of the document, which guarantees its integrity and identifies its signatory and shows his/her agreement to the content of the document (article 1322-1 §3 of the Luxembourg Civil Code).

To be valid as a signature, an electronic signature has to be created by a secured system based on a qualified certificate that the signatory can maintain under his/her sole control (article 13 of the law of 14 August 2000 relating to the ecommerce, as amended).

According to article 2 §1 of the Luxembourg Regulation of 1 June 2001 on electronic signatures, qualified certificates must contain:

---


450 see page 3: http://www.legilux.public.lu/leg/textescoordonnes/recueils/COMMERCE_ELECTRONIQUE/SIGNATURE_ELECTRONIQUE.pdf


452 Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement
an indication that the certificate is issued as a qualified certificate;
- the identification of the certification-service-provider and the State in which it is established;
- the name of the signatory or a pseudonym, which shall be identified as such;
- signature-verification data which correspond to signature-creation data under the control of the signatory;
- an indication of the beginning and end of the period of validity of the certificate;
- the identity code of the certificate;
- the advanced electronic signature of the certification-service-provider issuing it.

Pursuant to article 3 §1 of the Luxembourg Regulation of 1 June 2001 on electronic signatures, certification-service-providers (hereinafter referred to as “CSPs”) must:

- demonstrate the reliability necessary for providing certification services;
- ensure the operation of a prompt and secure directory and a secure and immediate revocation service;
- ensure that the date and time when a certificate is issued or revoked can be determined precisely;
- verify, on production of an official document of identity, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;
- employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognized standards;
- use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;
- take measures against forgery of certificates and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;
- maintain sufficient financial resources to operate in conformity with the requirements laid down in the applicable laws and regulations, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;
- record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;
- not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;
- use trustworthy systems to store certificates in a verifiable form so that:
  o only authorised persons can make entries and changes,
Qualified certificates issued by a CSP established within the EU have the same effect as those issued by a CSP established in Luxembourg. As for the qualified certificates issued by a CSP established in a non-EU country, they only have the same effect that as those issued by a CSP established in Luxembourg if one of following requirements is met (article 28 of the law of 14 August 2000 on ecommerce, as amended):

- the CSP fulfills the requirements of the Luxembourg law and has been accredited by a EU member state; or
- a CSP established within the EU has guaranteed the certificates issued by the CSP; or
- the CSP is recognized in the context of a bilateral or multilateral treaty with Luxembourg.

Any CSP has to notify to the Ministry in charge of eCommerce that its activities comply with these requirements (article 2 §1 of the Luxembourg Regulation of 21 December 2004 organising the notification of the CSPs).

Moreover, CSPs are free to apply for an accreditation (article 30 §1 of the Luxembourg law of 14 August 2000 relating to the ecommerce, as amended).

The accreditation is granted by the Ministry in charge of ecommerce, on the proposition of the Luxembourg Institute of the Normalization and Accreditation ("Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services" – "ILNAS") and on opinion of the Electronic Signature Committee ("Comité Signature Electronique").

As for secure signature-creation devices, they must, by appropriate technical and procedural means, ensure at the least that (article 4 §1 of the Luxembourg Regulation of 1 June 2001 on electronic signatures):

---


456 see footnote No 4.
the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
- the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
- the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

Besides, they must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

The Ministry in charge of the normalization\textsuperscript{457} publishes in the Luxembourg official journal (“\textit{Memorial}”) the references of the commonly admitted norms or technical regulations related to qualified certificates, CPSs and electronic signatures devices, except those already published in the Official Journal of the European Union (articles 2§3, 3§2 and 4§3 of the Luxembourg Regulation of 1 June 2001 on electronic signatures\textsuperscript{458}).

No norms or technical regulations have however been published in the Memorial in this respect since then.

According to the information available on the website of OLAS (“Office Luxembourgeois d’Accrédiation et de Surveillance”), i.e. the entity which had the powers granted to INLAS since 1\textsuperscript{st} June 2008, the following documents related to CSPs are currently eligible to be published in the Memorial\textsuperscript{459}:

<table>
<thead>
<tr>
<th>ETSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>TS 101 456</td>
</tr>
<tr>
<td>TS 101 733</td>
</tr>
<tr>
<td>TS 101 861</td>
</tr>
<tr>
<td>TS 101 862</td>
</tr>
<tr>
<td>TS 102 042</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWA 14167-1</td>
</tr>
</tbody>
</table>

\textsuperscript{457} Currently, the Ministry of Economy and External Commerce (Ministre de l’\'Economie et du Commerce Extérieur)

\textsuperscript{458} see footnote No 4

\textsuperscript{459} \url{http://www.olas.public.lu/legislation/reglementations/index.html}
Electronic Signatures

| CWA 14167-2 | Cryptographic Module for CSP Signing Operations -Protection Profile (MCSO-PP) |
| CWA 14168 | Secure Signature-Creation Devices Version EAL4 |
| CWA 14169 | Secure Signature-Creation Devices Version EAL4+ |
| CWA 14170 | Security Requirements for Signature Creation Applications |
| CWA 14171 | Procedures for Electronic Signature Verification |
| CWA 14172-1 | EESSI Conformity Assessment Guidance Part 1 - General |
| CWA 14172-2 | EESSI Conformity Assessment Guidance Part 2 - Certification Authority services and processes |

- **Technical conditions required in practice**

On 17 November 2008, the Luxembourg government launched a new website “www.guichet.lu” (hereinafter referred to as the “Counter”). The purpose of this new Internet portal is to offer a virtual Point of Single Contract to complete online all proceedings and formalities in relation with the Luxembourg administrations within the next few years. The Counter does not aim at replacing the traditional physical counters and offices.

The scope of the Counter is broader than that of the PSC in the meaning of the Services Directive since the Counter is not limited to the access to a Service and to the exercise thereof.

The Counter is divided into two main sections: one for citizens and one for businesses.

So far, only the so-called “citizen section” has really been developed as an online interactive platform for administrative formalities enabling not only to download documents but also to file them online and to send them to the administration by secured electronic means.

Besides this new application, the Luxembourg government has launched an eTVA application which enables to declare VAT online and an online service enabling to declare a new employee to the health Security.

In all cases, where it is possible to send to the relevant administrations an online form, if need be together with electronic documents, a PKI certificate delivered by Luxtrust S.A. is required.

---

4. [www.luxtrust.lu](http://www.luxtrust.lu)
Luxtrust S.A., which is a public-private partnership involving the Luxembourg government, the Chamber of Commerce of Luxembourg as well as various banks and other public entities, has developed the three following PKI certificates:

- the LuxTrust Smartcard, which is card equipped with a chip that contains two “electronic certificates”: one certificate reserved for the authentication or the protection of electronic communication and one certificate for the electronic signature;
- the LuxTrust Signing Stick, which looks like a USB stick and has a chip containing two “digital certificates”: one is to provide proof of the identity of the signatory and secure his/her electronic correspondence, and the other is a digital signature;
- the Signing Server Certificate which consists in a single-use random passwords known as OTPs (One Time Passwords) will be sent to the user on the medium selected at the time of ordering: either via SMS to a mobile phone, or on a Token, a type of key fob with a small integrated screen (the SMS option is only available via Luxembourg mobile telephone networks).

At this stage, the above-mentioned eGovernement applications do not accept other CSPs. This should change as soon as the interoperability difficulties with the other CSPs’ solutions have been sorted out on a EU level. The Luxembourg Minister for the Civil Service and Administrative Reform (“Ministère de la Fonction publique et de la Réforme administrative”) is actively participating in the STORK (“Secure idenTity acrOss boRders linked”) project launched by the European Commission on 30 May 2008⁴⁶⁴ and is supporting initiatives of the EU to facilitate EU wide interoperability of electronic identities.

⁴⁶⁴ See http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4147
22.1.2 Electronic documents for the purpose of the implementation of the Services Directive

As already said, Luxembourg has not legislated in order to implement the Services Directive yet. The Luxembourg Government is however currently drafting a bill to implement the Services Directive. This project should be provided to the legislature end of 2008 or beginning of 2009⁴⁶⁵.

However, from a practical perspective, Luxembourg has already undertaken several steps in order to meet the requirements of the Services Directive. Several highly comprehensive contact points have indeed been created in order to provide entrepreneurs with the information necessary to enable them to do business in Luxembourg, namely:

- the “Centre des Formalités PME” created by the Luxembourg Chamber of Professional Trades (“Chambre des Métiers”), notably though its website⁴⁶⁶;
- the “Espace Entreprises” of the Luxembourg Chamber of Commerce, also though its website⁴⁶⁷;
- the “Guichet Unique PME” created on the initiative of 21 communes of the North of Luxembourg, together with the above-mentioned Chambers⁴⁶⁸;
- the “Portail Entreprises” available at www.entreprises.public.lu (hereinafter referred to as the “Business portal”) launched by the Luxembourg Government since November 2004.

The latter website should play the role of a PSC, within the meaning of the Services Directive, as it will be integrated to the website “guichet.lu” in the future.

The development of the Business portal has been planned in two steps:

- Step 1 (from 2002 to 2004) consists in building up a centralised informative platform meeting the needs of the public as regards the creation and the management of a business in Luxembourg, i.e. the informative level;
- Step 2 (after 2004) aims at creating a virtual and interactive portal in which the entrepreneurs will not only be able to find information but also to use online forms, and make online secured and personalized transactions with the Luxembourg public administrations, i.e. transactional level.

⁴⁶⁸ http://www.guichetuniquepme.lu/
The Business portal now consists of a real guide for setting up and running business in Luxembourg that enables the Service Providers to find and to perform all the different administrative formalities, including the forms to be filed.

It notably contains a section named “Procedures” which includes a very useful interactive diagram of the statutory requirements to set-up an enterprise\textsuperscript{469}.

Each step of the diagram is virtually linked to a specific page reminding the Service Provider how to find information, what are the legal provisions, the statutory requirements and formalities that should be done, and containing hyperlinks to the websites of the competent administrations and, where applicable, to downloadable forms.

However, at this stage, the Business portal does not function as a complete interactive platform yet. Indeed, apart from the possibility for a Service Provider to declare a new employee for health benefits\textsuperscript{470}, the Business portal does not yet allow to exchange electronic documents between the users and the administrations.

It is planned that the Business portal will be integrated into the Enterprise section of the Counter within a short time and be developed in this context as a complete interactive platform for eGovernment applications by mid 2009.

In this respect, the Luxembourg government has defined the following main technical requirements:

- in general, supporting documents have to be submitted in PDF form. Based on decisions taken in the Expert Group on the implementation of the Services Directive, CAdES/XAdES signed documents should be accepted. Studies concerning those formats have already started.
- all pdf documents have to be electronically signed (using advanced or qualified signatures) before being transmitted to the competent authorities;
- the validation check of e-signature(s) is done via OCSP calls or CRL lists;
- the maximum size of pdf documents is 5 Mo;
- “trusted time stamps” of all submitted e-documents is required. This service is provided by Luxtrust;
- the exchange format for data is XML through web services;
- the Business portal complies with the referential of the Luxembourg public websites\textsuperscript{471}.

\textsuperscript{469} \url{http://www.entreprises.public.lu/procedures/demarches_creation/index.html}
\textsuperscript{470} \url{www.entreprises.public.lu} or \url{https://www.services-publics.lu/assistants-entreprises/public-detr?ECITIZ_ACTIVITY_PATH=Usager&ECITIZ_PROCESS_ID=CCSS-DETR}
\textsuperscript{471} \url{http://www.eluxembourg.public.lu/actualites/2008/02/presentation-reno/index.html}
22.2 Specific document types

22.2.1 Extracts from commercial registers

The Trade and Companies Register ("Registre du Commerce et des Sociétés") is publicly and freely accessible online\(^{472}\) or via the Business portal\(^{473}\).

The Trade and Companies Register's website offers today information on Luxembourg based companies and allows users to request in particular extracts from the Trade and Companies Register in two ways:

Firstly, the user can request an extract on a paper format. He will be able to download a specific form that can be filled in with Acrobat Reader or in writing. Then, the form should be addressed to the Trade and Companies Register either by fax or by postal mail. The Trade and Companies Register will confirm the order and send its invoice. The user will receive the extract a few days after the order.

Secondly, the user can also request and receive online an extract of the Trade and Companies Register. For this purpose, the user has to create his/her own account containing its personal data and password. The user can also log in using his/her LuxTrust electronic certificate. He will be able to order any documents available on the Trade and Companies Register on its personal account. He/she shall thus fill in the form and confirm the request as well as authorizing the payment. As a result, the user can decide to receive the ordered extract by postal mail or as a PDF file in his/her online account.

Electronically extracts of the Trade and Companies Register are issued by the administrator of the Luxembourg Trade and Companies Register and electronically signed which authenticates their validity.

Moreover, according to the draft bill n° 5716\(^{474}\) that should be passed in the beginning of 2009, the electronic deposit of documents necessary to incorporate and register a company and of those that have to be published in the Trade and Companies Register will be possible soon.

\(^{472}\) See https://www.rcsl.lu/mjrcs/index.do?time=1228324805206
\(^{473}\) See http://www.entreprises.public.lu/index.php
\(^{474}\) Projet de loi relatif au dépôt par voie électronique auprès du register de commerce et des sociétés - See http://www.chd.lu/fr/portal/role/lois/detail.jsp?order=descend&project=0&mode=number&page=1
22.2.2 Criminal records

Extracts from the criminal records (casier judiciaire) only exist in paper form in Luxembourg.

As there is no criminal liability for legal persons under Luxembourg law, there are no criminal records regarding legal persons.

Individuals can obtain an extract of their criminal records by addressing a request to the office of the public prosecutor in Luxembourg-City. Luxembourg applicants must provide with either a birth certificate, a family record book (“livret de famille”), a certificate of nationality, a passport or a national identity card. However, foreign applicants can only supply a national identity card⁴⁷⁵.

As a result, no electronic document exists at this time. However, considering the number of requests for criminal records, Luxembourg is currently analysing the feasibility of a web service allowing the users to request through the PSC an electronic criminal record.

22.2.3 Extracts from professional registers

Professional registers are managed by numerous private entities or public-law institutions, such as professional organisations or orders. The two main professional registers are the craftsmen register⁴⁷⁶, handled by the Luxembourg Chamber of Commerce (“Chambre de Commerce”), and the Trade Enterprise en Liberal Profession Register, managed by the Luxembourg Chamber of Professional Trades (“Chambre des Métiers”).

If not registered automatically further to the delivery of a governmental business permit (“Autorisation d’établissement”) by the Ministry of Middle Classes (“Ministère des Classes Moyennes”), craftsmen have to fill in an affiliation form before starting their business. This form can be downloaded online⁴⁷⁷ but must be sent back to the Luxembourg Chamber of Professional Trades by post mail. The “craftsman’s card” (“carte d’artisan”) which prove the affiliation to the Luxembourg Chamber of Professional Trades only exists as hardcopy.

---

⁴⁷⁵ see [http://www.mj.public.lu/services_citoyens/casier_judiciaire/index.html](http://www.mj.public.lu/services_citoyens/casier_judiciaire/index.html)
⁴⁷⁶ [http://www.entreprises.public.lu/formulaires/creation_reprise/afficdm/Affiliation_cdm.pdf](http://www.entreprises.public.lu/formulaires/creation_reprise/afficdm/Affiliation_cdm.pdf)
As for the affiliation to the Chamber of Commerce, a certificate of affiliation\(^{478}\) (“Certificat d'Affiliation”) can be obtained following a request made by mail, fax or email. However, such certificate is made available only as paper documents.

Currently, no governmental plans exist to make the use of electronic documents mandatory or to encourage them further.

22.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form.

However, the expected launch of online tax declaration in the near future may change this situation since certain insurance premiums are subject to tax deduction. The Luxembourg government is working on that since it is not only focusing on documents/certificates/attestations issued by government bodies but intends to involve the private sector as well.

22.2.5 Proofs of qualifications

Under certain circumstances, academic diploma have to be registered into a register of higher education titles\(^{479}\) (“Registre des titres d'enseignement supérieur”) or have to be recognized\(^{480}\) (“homologation”) by the Ministry of Culture, Higher Education and Research (“Ministère de la Culture, de l'Enseignement supérieur et de la Recherche”).

In both cases, the request must be introduced in writing and must include in particular a certified copy of the original diploma. In addition, all the requested documents must be written either in French, German or Luxembourg or translated into one of these three languages by a sworn translator in Luxembourg. The stamp of the translator must be affixed partly on both the translated text and partly on the document submitted for translation.

---


Thus, this procedure cannot be performed online, unless significant amendments of the legislation are brought into effect.

22.2.6 Statements from the service provider

The planned enterprise section of the Counter will be based on three levels of navigation: start from a theme, navigation down to sub themes, for finally ending up at the lowest level of the procedure (where the relevant forms can be accessed from). Each procedure will be described in the same manner. A fact sheet will sum up the objective of a procedure, it informs the user on which governmental body or agency is in charge of the matter, and, what events may trigger the procedure. It also informs on possible prerequisites and on how long the procedure will take. It also mentions the costs if any and gives a detailed description of the procedure itself, with legal references as well as links to electronic forms and electronic services when available.

As mentioned above, the Service provider will be required to use a Luxtrust certificate for any of its statements. The statements will be made under a web-form. Concerning the documents to be provided by the Service provider to support its statements, if they are only available in paper form, they need to be scanned, attached to the relevant electronic form and transmitted via the PSC to the competent authority. If the necessary documents are readily available in electronic form they will be managed in the “personal space” of the Service Provider and used in the relevant procedure.

22.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

22.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

Regarding the identification of the relevant public administration in charge of a specific task, the Business portal has already completed a huge and deep work in order to list the competent administration and the people to be contacted for each specific formality. Indeed, the Business portal uses hypertext links referring back to each relevant public administration and to details of the person to be contacted.

The PSC will remain a public service, under the responsibility of the Ministry of Economy. The communication mechanisms between the PSC and the public administrations will be defined uniformly at a national level and should not rely on individual delivery mechanisms.

The communication between the PSC and the competent public administrations has already been organised in the context of the existing Counter and will work in the same way for the enterprise
section of the Counter. Thus, an electronic workflow is put in place in order to orchestrate the handling of the process when necessary. Web-services or SOAP are used to exchange data based on XML standards. Each person responsible of the communication with the PSC have to be authenticated by a Luxtrust certificate.

22.3.2 The front-office – communication between the Point of Single Contact (PSC) and the Service provider

It is already planned that the enterprise section of the Counter will work like the citizen section of the Counter.

The Service provider will thus have to be authenticated by a Luxtrust certificate to have access to electronic and depositing assistants, that will enable it to find and carry out the relevant online formalities.

The duly authenticated Service provider will have an exclusive access to its “Personal space” ("Espace personnel"), which will be organised as a virtual locker and which will enable the duly authorised Service provider to communicate with the administration, to fill in online forms and also to store its documents and requests. The personal space of the Service Provider will indeed be divided in two sections: its personal details and its folders. The personal details section will store all the relevant information about the Service user that it may regularly have to provide to the administrations. Electronic assistants will then automatically use these data to fill other forms. The folders section will store all previous and current administrative procedures made by the user. Therefore, the user will always be able to consult, to save as a pdf file or to print the documents he/she has previously provided to the administrations through the Counter.

From a legal perspective, it remains necessary to define the access rights to e-services for businesses. Delegation of signature, mandate from beneficiary, etc. have to be clearly defined. The Luxembourg government is currently working on those aspects.

22.3.3 The front-office – communication between the Government and the Service provider

As mentioned above, the Service provider and the Government will be able to communicate through the PSC via the Personal Space application.

The Service provider will thus be able to receive emails and notifications from the public administration via its Personal space under the above-mentioned protocols and secured means.

However, in general, any electronic communication that the Service user will receive from the relevant administration though its Personal space on the PSC will be followed by a written notification.
It is agreed upon that the Service provider receives at least two notifications on its Personal space: an acknowledgement of receipt of its request and a notification that its request has been treated.

The Luxembourg government is also currently working on an e-delivery solution for certain attestations and certificates. Such electronic delivery of official documents would need legislative amendments in most cases.

22.4 Assessment – Plans, progress and proposals for further harmonisation

22.4.1 Current plans and progress in the implementation of the Services Directive

As shown in the overview above, Luxembourg has already developed an advanced online infrastructure in a view to the implementation of the Services Directive, in the form of the website www.entreprises.public.lu which already assumes certain functions expected from the PSC, notably the providing of information to the Service provider and the centralisation of the procedures of creation of a Service. The content of this website will be integrated in a near future to the Counter, which is already ready to play the role of the PSC.

Luxembourg has also already put in place a complete online procedure for the declaration of VAT, i.e. the above-mentioned eTVA application as well as an electronic procedure for declaration of employment. The electronic means of authentication, including electronic signature, used in the eTVA application and the other interactive applications accessible to individuals on the Counter, will serve as a firm foundation for the development of the PSC within the meaning of the Services Directive.

According to the Luxembourg national reform program\(^{481}\) adopted by the government on 17 October 2008, the launch of an electronic assistant for the creation of enterprises is being finalised and should be launched in the course of 2009. This new tool will enable the Services providers to create their enterprise online, through a totally electronic procedure. It will notably cover not only the common business permit ("autorisation d’établissement") which concerns the running of commercial activities but also more specific business permits as those related to travel agencies or to certain liberal professions for instance. At last, the eTVA application will be integrated to the Counter as well as the electronic filing with the Trade and Companies Register.

This new online tool for the creation of enterprises will not replace the two main current physical points of single contacts which are the Luxembourg Chamber of Commerce and the Luxembourg Chamber of Professional Trades. It therefore remains unclear how the websites of these Chambers, which already provide a huge amount of information relating to the creation of a Service and also contain hyperlinks to the relevant administrations, will progress in the future.

Finally, it needs to be underlined that Luxembourg grants a high importance to the modernization of its administrations and of its administrative services in general, and their evolution towards a coherent, comprehensive and efficient electronic management. The executive plan for the Public eGovernance482 previously enacted by the Luxembourg government notably insists on the importance of the interoperability of national administrative and public services among themselves and also with the international and, especially European administrations.

22.4.2 Suggestions for further European support initiatives

As stated above, with regard to electronic signatures, Luxembourg now has given its preference to the PKI certificates delivered by Luxtrust as a mean of authentication of the users of eGovernement applications.

The Luxembourg government will however accept other certificates for the eGovernement applications once the interoperability issues have been solved at an European level.

482 http://www.eluxembourg.public.lu/eLuxembourg/plan_directeur/plan_directeur.pdf
23 Malta

23.1 General framework for electronic documents in eGovernment applications

23.1.1 Electronic documents in eGovernment applications

At present, beyond the direct transposition of the relevant provisions of the Services Directive, the e-Signatures Directive and the e-Commerce Directive, Malta does not have a generic framework related to the use of electronic documents in eGovernment applications – neither from a legal perspective nor from a technical or procedural point of view.

Indeed, whilst a considerable array of electronic Government applications and services are available to the public in Malta, they remain regulated and implemented on a case by case basis and subject to the strategy and/or policy applicable at the time. Thus there is no sui generis law which regulates the legal framework and/or the technical or procedural aspects of the use of electronic documents in e-Government.

Maltese e-government applications can be sub-divided into two streams. The first stream refers to those which can be accessed online but which do not require any authentication. The second stream refers to a number of applications which require authentication and/or electronic signature. Therefore the services which mostly concern this survey are those related to the second stream, that is, those which as such necessitate a legal, procedural and infrastructural framework (including a single point of contact) which should allow such services to be offered, maintained and delivered on a cross-border basis in accordance with the Services Directive.

Currently e-government services in Malta can be accessed via a common web portal. Maltese citizens can access the “mygov.mt” portal and log in to his/her own account by using an Electronic Identity (e-ID) which is considered as falling under the definition of ‘electronic signature’ under the Electronic Commerce Act. Maltese citizens are entitled to obtain a free e-ID which allows substantial easy access to the specific e-government services which require prior authentication as aforesaid. Certain other e-government services require a higher level of authentication – in which case users who wish to use such services are required to use a non-qualified Digital Certificate prior to accessing the service. This too is freely available to the citizen. The next (third) phase of e-government in Malta is intended to


484 Chapter 426 of the Laws of Malta of 2002

introduce electronic Identity Cards which in turn would offer increased protection and security when compared to the e-ID and the non-qualified digital certificate.

Therefore, the current e-government system is based on prior authentication of the transacting parties and/or the signing of a transaction per se rather than the signing of individual electronic documents used in a transaction. For instance where an identifiable entity enters the system to use an electronic service and is authenticated by means of his e-ID and is subsequently required to submit a form, that entity is at present not required to sign the form. The reason behind this is that the identifiable entity has been authenticated prior to accessing the electronic service and the transaction is seen as authenticated to this extent. Note however that at the moment e-government services in Malta are only available to private individuals, although the provision of such services to and by organisations amongst others is in the pipe-line and is planned to be launched in the near future.

In Malta there is an increasing general practice (or a somewhat custom-type regulation) of using electronic forms in e-Government which are until today unregulated (in terms of technical and procedural requirements and standards) and are generally completed in HTML format. In fact Malta is currently moving towards establishing a uniform e-government framework which functions on an electronic Forms server-based engine - “MyForms”. The aim is to deploy a user-friendly mechanism allowing any new electronic government service which requires the transmission and exchange of data to be carried out by means of customised electronic forms reflecting the nature and requirements of that new service. This project appears to comprise three key steps – these being (i) reducing the number of forms by rationalising the data which is being collected and by eliminating redundant forms, (ii) making the forms available electronically with improved overall speed and efficiency of forms filling, routing and management and, (iii) ensuring the effective, secure interchange, processing and archiving of the forms based information that is generated by electronic commerce and administrative transactions.

The functionality will allow the authorised users to create the required eForms and publish them to the general public and shall retain a central repository of all eForm templates. This would operate via a simple web interface allowing the user and/or service provider to create a customized form which would be saved in a common standard format – most likely in an open XML standard which can in turn be rendered into a number of other formats (such as word/html/pdf, etc) and which would facilitate common archiving and re-traceability of the Forms. In addition it is projected that this would also facilitate the integration of a Work Flow system which would be integrated or attached to each form allowing real time tracking and follow-up of the form and of any activity or procedures related to the form.

Ultimately this should allow end-to-end management of electronic services by permitting that one entity/person can be responsible for reviewing the full process from accessing a service to final delivery and acceptance of the service.

The Malta ICT Strategy for 2008-2010 stipulates that an e-Government Shared Services platform is to be deployed through which a repository of shared services would allow entities to deliver services customized to the demand of their customers. The first eGSS is to be a unified content management system for government thus providing for myAlerts (a notification platform), the myForms online form processing repository and “mybills” - a single bill settlement web service for all entities. Although

---

485 “the Smart Island” - https://secure2.gov.mt/SmartIsland/Pages/Home.aspx
preparation for the latter is currently being undertaken no further information is available to the public in terms of launch dates.

Ultimately therefore, until today, there remains no single harmonized regulation of the latter proposed infrastructure although there are plans to develop some framework (likely to be soft law) which would regulate or at least provide certain guidelines on the infrastructure.

23.1.2 Electronic documents for the purposes of the implementation of the Services Directive

Malta appears to appreciate and value the principles of the Services Directive and is planning ahead to ensure proper, easy and quick acceptance and delivery of cross border electronic services. At this stage it is important to clarify that generally Maltese e-government services are easily accessible and can be accessed/seen by a user prior to being authenticated via an e-ID which means that as such any non-Maltese citizen who wishes to view a service need not necessarily have an e-ID account.

In relation to the acceptance of electronic documentation by the Maltese authorities, the projected plan is for non-Maltese citizens to be able to access electronic services online and to complete the service online. Therefore, where necessary, the foreign citizen shall be able to;

1. download or upload any electronic documentation; and
2. complete the form electronically or manually; and
3. attach any necessary documents to the completed form; and
4. scan or save the form and attached documents into electronic form; and
5. sign the form and attached documents; and
6. submit by electronic means the signed form and documents to the Maltese administration through the Single Point of Contract (note that at present the appropriate electronic channel for submission and the technical standards and requirements have not yet been determined).

Specific legal requirements have not yet been defined in relation to document types, formats or signatures. Nevertheless Malta is likely to implement a “soft-law approach” which would aim at harmonizing the use of electronic documents in e-government rather than imposing single standardized requirements. The same applies in relation to technical requirements whereby it is likely that guidelines will be issued in terms of standards and specifications which ought to be employed.

In terms of the setting up a Point of Single Contact (PSC) Malta is moving towards the implementation of one singular Point of Contract in accordance with Article 8 of the Services Directive. This idea therefore is to set up the PSC to function as a singular entity through which national or foreign service-providers can access all service activity and submit to and complete all end-to-end procedures and formalities relating to that service at a distance and by electronic means.
Although still at planning stage, the concept shall be that of establishing this singular entity (in parallel with the idea of creating the uniform eGSS platform) which would itself transact by means of the e-government platform as though it was the client – thus applying for and following through the full process until the electronic service is delivered and accepted. To this end however, details of the framework which shall provide for guidelines and/or statutory provisions to regulate the PSC and its activity are still not available to the public domain.

### 23.2 Specific document types

#### 23.2.1 Extracts from commercial registers

Extracts from commercial registers in Malta are available from the Malta Financial Services Authority (MFSA) website[^486]. The MFSA is the single regulator for financial services activities in Malta. It regulates and supervises credit and financial institutions, investment, trust and insurance business and also houses the country's Companies Registry[^487].

The MFSA retains a number of details relating to companies and other commercial entities, including for example (i) Entity name and legal structure (ii) Company Registration numbers (iii) Business Addresses (iv) Date of establishment (v) Memorandum and Articles of Association and (vi) Good Standing Certificates. Some of this information is publicly accessible and searchable online whereas others may be subject to a fee or payment.

The MFSA also provides various services which are regulated according to law and which therefore require adherence and conformity with various procedures and requirements stipulated by law. These services include amongst others:

1. Registration of new commercial partnerships
2. Registration of documents related to commercial partnerships
3. Keeping the company and partnership register
4. Collection of registration and other fees
5. Publication of notices
6. Issue of certified documentation
7. Issue of good-standing and other certificates
8. Reservation of company names

9. Imposition and collection of penalties
10. Investigation of companies

Some of these services can be carried out online by means of the recently implemented Registry of Companies (ROC) Online System which uses Secure Socket Layer (128-bit SSL) protocol to encrypt information and allows electronic forms to be filed and signed electronically using a personal digital certificate. Currently the few documents available for electronic filing are company Annual returns, Memorandum & Articles of a company, and two forms (the Form T and Form K) – thus allowing new companies to be set up online. It is expected that a new electronic Form (Form Q) shall be launched by the second quarter of 2009 allowing users to change or amend registered addresses online.

In terms of filing of the aforementioned electronic documents the Authority has established an internal policy which was intended to provide sufficient security in terms of authentication and verification depending on the nature of the transaction being carried out.

The structure of the system was designed with a scaled security process in mind, whereby the user is required to first inform the MFSA’s registry (by means of an application) that the user wishes to use a Digital Certificate which he/she possesses in order to be able to carry out certain transactions. The technical system employed by the Authority is equipped to accept and process any form of Digital Certificate which is acceptable to the standards required by the registry. However, at present the Authority only accepts Digital Certificates issued by the government of Malta via the e-ID system. Nevertheless it is expected that the Authority should be accepting other Digital Certificates by the second quarter of 2009 as long as such Certificates are up to the standards required by the Registry – that is at minimum a Class II Digital Certificate which requires a one-time physical representation of the user prior to acquiring the Digital Certificate.

Apart from requiring username and password verification and the use of such Digital Certificate, the Authority’s internal policy requires and/or permits the Registry to carry out stricter authentication processes. The technical system will confirm whether the Digital Certificate being presented is valid and according to the required specifications and/or standards. In addition the registrar at the Authority may employ a specific Module which allows him to verify the certificate manually and where necessary he may request further documentation or evidence as may be required.

Once approved by the ROC as a system user, the user can register his/her Digital Certificate with the ROC Online System, following which the user can start creating and submitting electronic forms online for the companies he/she has been authorised by (via the ROC Online System accompanied by a written consent from the company). To this end, an increased authentication procedure requires the user to request approval from the authority to carry out various transactions or to make use of certain services. For instance, if a user wishes to sign on behalf of a Company he will need to first obtain approval of his digital certificate and then need to obtain approval from the Registry authorising him to sign on behalf of the Company. Such authorisation is only issued by the Registry once it confirms that the applicant is indeed a valid legal representative of the company (such as a Director or Company Secretary) or that he has been legally and validly authorised by the Company to act for or on behalf of the Company.

As stated above, such security and authentication framework is not specifically regulated by law except in as far as the e-Commerce Act regulates the use of electronic signatures and certificates. It
appears that until today the whole process was prepared, designed and set-up by the MFSA according to the needs of the MFSA and which therefore did not fall under the central e-government structure *per se*. Nevertheless the intention is that of integrating these procedures and requirement under the single myForms structure. It must be noted also that in terms of time-stamping, such activities remain unregulated in Malta and at present there exist no obligations, requirements or guidelines in this regard. In fact the MFSA does not use or require time-stamping.

23.2.2 Criminal records

Maltese citizens can request a copy of their Police Conduct from the police which are issued subject to the provisions of Chapter 77 of the Laws of Malta (*the Conduct Certificates Ordinance*).

In practice the issuance of such certificates is done only in paper format although as such nothing at law prohibits their issuance in electronic format.

Nevertheless, it appears that at present the procedure (which does not appear to emerge from the law) for applying for the certificate necessitates the requesting individual to collect the certificate personally. Where this is not possible it can be collected by a close relative only if the ID Card of the applicant and of the relative is presented together with an authorization letter authorizing the relative to collect the certificate which is to be endorsed with the signature of the applicant. In addition, in those cases where the Conduct is requested for local use or for use within one of the EU Member States the Maltese ID card is needed; in the case of use in third countries the Passport of the applicant is also required.

As already stated, there does not seem to be any legal framework which as such requires physical presence of the applicant. Indeed, the plan is that such documents should in the near future be made accessible in an electronic format and it is likely that this shall be done by using the Forms system referred to above and that the technical standards for such forms shall be XAdES. However specific measures and/or standards have not yet been published in this regard and it is not yet clear whether this shall be a mandatory obligation or not. Moreover, time-Stamping activities also remain unregulated in Malta and there are no obligations, requirements or guidelines in this regard. Moreover, Malta is considering any recommendations which may be published by the European Commission so as to ensure as much procedural and technical cohesion and interoperability between systems as is possible.

23.2.3 Extracts from professional registers

In Malta extracts from professional registers are generally issued in paper form. Although it is not possible to give a complete overview of all professions in Malta it can be said that in accordance with the e-Commerce Act there is nothing which should prohibit such documents from being distributed electronically.
Nevertheless, the plan in Malta is that such documents should in the near future be made accessible in electronic format and it is likely that this shall be done by using the forms system referred to above. As already stated, Malta continues to take into consideration recommendations and/or proposals being made at EU level and thus continues to consider the implementation of XAdES as a possible technical solution in this regard. Indeed, specific measures and/or standards have not yet been published in this regard and it is not yet clear whether this shall be a mandatory obligation or not. Moreover, Malta is considering any recommendations which may be published by the European Commission so as to ensure as much procedural and technical cohesion and interoperability between systems as is possible.

23.2.4 Certificates of insurance

In Malta certificates of insurance are generally issued in paper form although, as in the case of the commercial and criminal records, there is nothing in the law which legally prohibits their issuance in electronic form (as in fact they would be legal in terms of the Electronic Commerce Act).

We do note however that some insurance agencies do offer a few services online – primarily the sale of short-term travel insurance policies (which permit a lower level of underwriting compared with other forms of insurance policies) whereby the policy is issued in electronic form however without any use of electronic signatures and/or digital signatures in the procedures.

At present, in relation to the issuance of such documents to the Maltese administration (or generally) no plans have been finalised which mandate the issuing of the documents in electronic form or which stipulate standards or technical requirements in relation to their acceptance, format or signature. Notwithstanding, the intention is to encourage and allow such service providers to have access to the applications offered via the mygov portal thus allowing and encouraging service providers and users to offer services online (as approved organisations) with improved verification, authentication and security levels in place and which would hence give such organisations access to the MyForms system referred to above. In essence, the system would allow entities to sign into the e-ID system permitting to offer services via the mygov portal as an approved organisation. Once having signed on the service provider will then be able to create and use the e-Forms as discussed above.

23.2.5 Proofs of qualifications

In Malta the general practice remains that proofs of qualifications are only issued in paper form by the issuing entity. While electronic copies might occasionally be presented in the form of unsigned scans procedures are not generally carried out electronically.

Whereas no legislation, framework or guidelines exist for electronic proofs of qualification beyond what is available in the Electronic Commerce Act, the intention is that the above mentioned standardised framework will allow such documents to be delivered and received electronically in...
various formats (such as Word or PDF format and which would be uploaded and transmitted via the Web Form system described above.

23.2.6 Statements from the service provider

The plan for statements is that of having a standardized framework which will also allow the use of digital signatures and the MyForms system referred to above. This would mean that the service provider will be allowed to issue statements most likely by uploading the form via the MyForms systems in one or more authorised formats (such as PDF or Word) and signed and uploaded via the Web Form.

Although the framework has not been finalised yet, Malta is looking out for developments and/or guidelines being issued from the European Commission’s side and will seek to implement any proposals made by the Commission (which thus far appears to be leading to XAdes standards being implemented in this regard).

23.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

23.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As mentioned above, it is likely that Malta will set up and implement a Point of Single Contact which shall allow the administration or private entities to apply for the service online and have the service delivered online directly via the PSC. Thus it is expected that the PSC shall be able to follow the complete process – an end-to-end solution. It is also expected that this framework shall be based on the Electronic Forms based engine for all services (although in the short term this could start off by employing an individual approach directed at specific services before transforming all services into electronic form in a phased manner).

In terms of how the technical and organisational aspects behind the process are to be handled one must understand that due to the relatively small scale of Malta, the project of implementing a single point of contact should be easier and should be facilitated by a straightforward delegation of tasks and responsibilities. To this end, it is expected that each organisation and/or administration will have a
single key Contact Person who is responsible for the interaction with the PSC and who would be obliged to inform and co-ordinate any changes or developments with the PSC.

With this in mind, although in reality there is nothing at law which prohibits the delivery of electronic mechanisms in view of the PSC there remains a need to change the current framework and to regulate the mechanisms further. In fact, at present Malta is undergoing a detailed process to introduce a cutting down of over-burdensome or bureaucratic procedures which are still required at a manual level and to introduce instead simplification and scaling of processes which can be sealed and adhered to easily in an online and interconnected environment. Once again, the aim is to employ the web-based Forms system which shall allow foreign users to access the system using a Digital Certificate and hence to upload and transmit the electronic Forms online. Indeed however at present there is a lack of guidance or regulation of key elements which need to be somewhat clarified including technical standards to be used and more generally regarding the use of languages, and liability of all parties involved amongst other things.

23.4 Assessment – Plans, progress and proposals for further harmonisation

23.4.1 Current plans and progress in the implementation of the Services Directive

Malta is currently holding discussions and negotiations with other EU Member States so as to pre-empt as far as possible any severe divergence of approaches, methods or formats employed by the members states and thus to promote and encourage interoperability of systems from an administrative, procedural and technical perspective in as far as is practical. These discussions show that there is a will to encourage mutual recognition of documents on a cross-border level in terms of the Electronic Services Directive.

Ultimately, Malta is itself moving away from its previous multi-silo approach to one which is more integrated and uniform allowing the sharing of services of and information. The Point of Single Contact is intended to allow all EU citizens access to electronic services offered in Malta which should be available, accessed and delivered from one single portal. To this end, Malta notes that as the process to streamline and simplify traditional processes is going on it shall continue to carry out consultation processes with Maltese stakeholders in this regard so as to ensure that service providers can provide and gain access to services online easily and without undue delay. One therefore awaits the launching of the 3rd phase of e-government services together with the launch of the ‘organizations’ functionality on the e-government platform, the launch of the Point of Single Contact and the launch of the eGSS unified content manager which should bring together a tighter platform for e-services.

23.4.2 Suggestions for further European support initiatives

Malta views the aforementioned eForm project as that which should in the long term satisfy the requirement of Article 8 under the Services Directive in relation to EU Citizens (not being Maltese
citizens or Maltese residents). However this remains subject to a number of crucial technical and policy developments that still need to occur at local level and at the European level.
24 The Netherlands

24.1 General framework for electronic documents in eGovernment applications

24.1.1 eGovernment applications in general

general framework for electronic documents

Dutch law provides a generic framework related to electronic documents in eGovernment applications in the General Administrative Law Act ("Algemene wet bestuursrecht" (Awb)). Section 2.3 Awb allows electronic communication ("verkeer langs elektronische weg") between individuals and administrative authorities ("bestuursorganen") provided that the provisions in this section are observed (article 2:13 paragraph 1 Awb). The administration is allowed to send electronic messages in case a citizen has stated that he is sufficiently capable of accessing them by electronic means (article 2:14 paragraph 1 Awb). Furthermore, the issuing of electronic messages should be sufficiently reliable and confidential (article 2:14 paragraph 3 Awb).

Citizens may send electronic messages to an administrative authority to the extent that the existence of this possibility has been announced by the administrative authority involved. The administrative authority can set specific requirements to the use of electronic means of communication (art. 2:15 paragraph 1 Awb).

The administrative authority is obliged to confirm receipt of electronic applications (article 4:3a Awb). When no legal requirements exist, the competent administrative authority may prescribe the use of specific forms for submitting an application and information (article 4:4 Awb).

specific requirements for electronic signatures

Specific requirements with regard to electronic signatures have been set in the Telecommunications Act ("Telecommunicatiewet"), the Electronic Signature Act ("Wet elektronische handtekeningen")\textsuperscript{488}.  

\textsuperscript{488} Act of 8 May 2003 amending Book 3 and Book 6 of the Civil Code, the Telecommunication Act and the Economic Offenses Act with regard to electronic signatures (Wet van 8 mei 2003 tot aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad
the Electronic Signature Regulation ("Regeling elektronische handtekeningen")\textsuperscript{489} and the Electronic Signature Decision ("Besluit elektronische handtekeningen").\textsuperscript{490}

If a signature is needed in dealings with the administration, an electronic signature can be used, provided that the authentication method used is sufficiently reliable, taking into consideration the content and the purpose of the message (article 2:16 Awb). Article 3:15a and 3:15b of the Dutch Civil Code ("Burgerlijk Wetboek (BW)") are applicable. Article 3.15a BW provides a number of conditions that should be met in order for the used authentication method to be deemed sufficiently reliable. Article 3:15b BW regards the validity of electronic certificates.

The requirements mentioned above primarily regard the electronic messages as such and the use of electronic signatures, not the documents contained therein. Section 2.3 Awb does not provide any specific requirements regarding electronic documents, nor any other technical or procedural requirements.

Administrative law regularly requires documents to be issued in writing. For example, the application for an administrative decision ("aanvraag voor een beschikking") and the administrative decision itself should be set out in writing (article 4:1 and 1:3 paragraph 1 Awb). However, this principle does not hinder the use of electronic means of communication since the term "in writing" is broadly interpreted within section 2.3 Awb.

\textit{technical requirements in soft law}

Recently, the Dutch government has adopted the program "Netherlands in open connection", regarding the stimulation and adoption of open standards ("Actieplan Nederland Open in Verbinding"). The program aims at promoting the use of open standards and open source software in government administrations when using ICT to expand interoperability between (government) organisations and to reduce dependency on software providers.\textsuperscript{491} In the context of this program, an overview of open standards was published, which can be used as a checklist by individuals, companies and administrative bodies to implement open standards, develop an ICT strategy and to establish

\begin{footnotesize}
\textsuperscript{489} Regulation published by the State Secretary of Economic Affairs of 6 May 2004 (Regeling van de Staatssecretaris van Economische Zaken van 6 mei 2003, nr. WJZ/03/02263, houdende nadere regels met betrekking tot elektronische handtekeningen).

\textsuperscript{490} Decision of 8 May 2003, containing requirements for the rendering of services with regard to electronic signatures (Besluit van 8 mei 2003, houdende de vaststelling van eisen voor het verlenen van diensten voor elektronische handtekeningen).

\textsuperscript{491} See http://www.forumstandaardisatie.nl/lijst-open-standaarden.
\end{footnotesize}
24.1.2 Electronic documents for the purposes of the implementation of the Services Directive

acceptance of electronic documents

The acceptance of electronic documents, including from other Member States and EEA Countries is regulated in article 4, paragraph 1 of the Services Act. Here it is stated that a competent authority to which a service provider or a recipient submits information or documents to prove that a condition has been met or a permit has been acquired, will also accept:

a. information and documents from another member state that serve a similar purpose or that show that a condition has been met or a permit has been acquired.
b. harmonised forms in the sense of article 5, paragraph 2 of the Services Directive.

When applying article 4, paragraph 1, a competent authority is only allowed to require an original copy, a certified exact copy or a certified translation of original copies if this follows from a treaty of the European Union or from a binding decision of an institution of the European Union, or if this is required by overriding reasons relating to the public interest.

Competent authorities should see to it that messages and documents of services providers regarding procedures and formalities can be easily send to them through the PSC (article 14 paragraph 1c Services Act). Furthermore, administrative authorities may not refuse to accept information or documents that have been sent through the PSC based on the argument that this would lead to a disproportionate administrative burden for them (article 15 paragraph 1 Services Act). These obligations benefit all national and foreign service providers that fall within the scope of the Services Act.

It is noted that the number of authentic documents needed for the handling of procedures and formalities, will most likely be very limited. Most procedures and formalities do not seem to require the use of authentic documents.

Within the context of administrative cooperation as provided for by chapter VI of the Services Directive - which has been transposed in Chapter 6 of the Services Act – no specific legal or technical requirements have been set for the use of electronic documents. The Netherlands are not aware of any technical specifications or limitations within the Internal Market Information System (IMI) regarding...
electronic documents and the exchange of such documents between the competent authorities through IMI.

**specific legal and technical requirements**

Specific technical requirements have been adopted with regard to digital documents which under the Archive Act ("Archiefwet") have to be archived in the official records of public authorities. These specific requirements have been adopted by the Ministerial Regulation orderly and accessible condition of records, based on the Archive Act. However, these specifications do not concern the service provider nor are they imposed on the service provider. They are specifically directed at the competent authority which receives documents and which by law has an obligation to archive such documents.

Other than the requirements mentioned above (see also eGovernment applications in general) no specific legal or technical requirements have been set.

**status of implementation Points of Single Contact**

On 13 December 2007 the Minister of Economic Affairs has informed the Dutch House of Representatives ("Tweede Kamer") on the implementation of the Services Directive ("Directive"). The implementation consists of three parts. Firstly, the main obligations resulting of the Directive will be implemented in the "Services Act" ("Dienstenwet"). The proposal for the Services Act has been adopted by the Council of Ministers and was send to the Dutch House of Representatives on 5 September 2008.

The second part of the implementation is contained in the Reform Act ("Aanpassingswet") that will adjust sector-specific regulations to meet the requirements of the Services Directive and the Service Act. The Reform Act will also implement certain obligations that could not be dealt with in the Services Act. According to expectations the proposal for the Reform Act will be submitted 6 months after the proposal for the Services Act.

---

493 Letter of the Minister of Economic Affairs, dated 13 December, 2007 to the Chairman of the House of Representatives of the States General.

494 An overview of all relevant documents related to the implementation of the Services Act can be found on the website of the Ministry of Economic Affairs. See http://www.ez.nl/Onderwerpen/Groeiende_economie/Dienstenrichtlijn.

495 Proposal regarding implementation of European regulations regarding the rendering of services on the internal market (Services Act ("Implementatie van Europese regelgeving betreffende het verkeer van diensten op de interne markt (Dienstenwet")).
Finally, a Catchall Act ("Veegwet") will be proposed that will repair any technical imperfections and omissions from the Services Act, the Reform Act or any other legislation that is related to the implementation of the Directive.

To ensure a timely and correct implementation of the Service Directive the Minister of Economic Affairs has created a Working Group on the Implementation Services Directive ("Projectgroep Implementatie Dienstenrichtlijn" (PID)), which consists of officials of the Ministry of Economic Affairs, the Ministry of Justice and the Ministry of the Interior and Kingdom Relations. This working group is responsible for the national coordination of the implementation.

Concrete steps to implement Points of Single Contact (PSCs) are included in the Services Act ("Dienstenwet"). Article 5 Services Act instructs the Minister of Economic Affairs to establish and maintain a Point of Single Contact for service providers and commercial recipients, referred to as the Central Desk ("centraal loket"). To service providers the Central Desk will provide (i) information needed to access and to exercise service activities and (ii) correspondence regarding procedures and formalities between service providers and competent authorities. To commercial recipients the Central Desk will provide information regarding the use of services in the Netherlands and other member states.

Pursuant to Article 6 Services Act the Dutch Consumer Authority ("Consumentenautoriteit") is responsible for establishing a Point of Single Contact for consumers, referred to as the Information Point ("Informatiepunt") that provides information regarding the use of services in the Netherlands and other Member States.

Both the Central Desk and the Information Point will be easily accessible by electronic means (article 5, paragraph 2 and article 6, paragraph 2 Services Act).

Together, the Central Desk and the Information Point form the PSC, in the Netherlands also referred to as the "One-counter" ("Eén-loket"). The One-counter matches existing e-government programs and stimulates the progress of such programs. The government intends to incorporate the Central Desk in the existing Business Counter ("Bedrijvenloket"), which acts as "front-office" for disclosing information and procedures to entrepreneurs. Currently, a substantial number of central and decentralized (government) institutions provides information through the Business Counter.496

By Order in Council, further arrangements with regard to the establishment, the maintenance, the functioning and the security of the Central Desk and the Information Point can be introduced (article 5, paragraph 3 and article 6, paragraph 3 Services Act). At this moment such an Order has not yet been published.

496 See http://www.antwoordvoorbedrijven.nl.
Noteworthy is also the obligation for competent authorities to be sufficiently accessible via the central point of contact for messages relating thereto from a service provider as provided for in Article 14, paragraph 1, under c), of the Services Act. Rules may be drawn up by ministerial order concerning the technical requirements which a competent authority must meet with a view to connecting to the central point of contact. At this moment such a ministerial order has not yet been published.

In recent years a number of efforts have been made to stimulate the use of electronic documents. One of these initiatives is a program called E-forms (E-formulieren) in which a large number of paper documents have been converted to electronic forms. These do not necessarily cover formal documents that need to be submitted with a procedure or formality. In some cases, access for citizens to these forms is granted through using a digital ID-system called DIGID.

In March 2008 a report on the feasibility of a timely implementation of the Service Directive was presented. The report gives an overview of the necessary efforts by decentralized government bodies and an estimate of the financial consequences thereof.

24.2 Specific document types

24.2.1 Extracts from commercial registers

Technical characteristics
In the Netherlands all key information related to economically active entities is registered in the trade register of the Netherlands Chamber of Commerce (“Kamer van Koophandel”). Registration in the trade register is compulsory for every company and almost every legal entity. The Chamber of Commerce issues electronic extracts from the Commercial Register. These extracts are issued in the form of certified electronic documents. These electronic documents contain a PDF-file that has been certified by the Chamber of Commerce, using a VeriSign certificate. The documents are sent to the applicant by email. The certificate is valid for 12 months. After this period the document can still be accessed but the electronic signature can no longer be verified.

Acquisition
The electronic extract can be acquired through the website of the Chamber of Commerce. To get access to the online trade register a code and a password are needed. These can be acquired on the

---

website. Searching the trade register is free of charge, but the Chamber of Commerce does charge costs for business extracts.

**Legal Framework**

The issuance of electronic extracts is based on article 22, paragraph 1 of the Commercial Registers Act ("Handelsregisterwet"). The use of the certificate is subject to a Trusting Party Agreement ("Vertrouwende Partij Overeenkomst") which determines the conditions on which and the extent to which the trusting party may trust the certificate issued by the Chamber of Commerce, acting as a Certification Service Provider ("CSP"). The degree of reliability of the electronic signature and the corresponding certificate are outlined further in a Certification Practice Statement (CPS).

### 24.2.2 Criminal Records

**Document Format**

In the Netherlands extracts from the penal register are not available to natural persons or legal persons. Such extracts are only available to the Public Prosecutors Office, the police and other specifically designated organisations and officials. The Judicial Data and Criminal Records Act governs the registry and information exchange of such information. However, the Netherlands can provide some information on the criminal record of a service provider by the possibility to issue a 'statement of conduct' ("Verklaring omtrent het gedrag" (VOG)). These certificates are only available in a paper format. The extract is provided to natural persons and legal entities by the Central Agency Good Conduct Certificates ("Centraal Orgaan Verklaring Omtrent het Gedrag" (COVOG)), which is an agency acting under the responsibility of the Minister of Justice.

**Acquisition**

Natural persons can apply for a statement of conduct by submitting an application form to the municipality in which they are registered in the Municipal Personal Records Database ("Gemeentelijke Basis Administratie" (GBA)). The municipal authority is responsible for the verification of the information provided by the applicant and for sending through the application form to COVOG. The applicant or its authorized representative is to furnish proof of identity. In case the natural person is not registered at any GBA, the application has to be submitted to COVOG directly.

Legal entities can apply for an extract to COVOG directly by submitting three application forms regarding (i) the natural persons involved, (ii) the legal entities involved and (iii) the applicant.

---

It should be noted that the obligations of administrative cooperation under Chapter 6 of the Services Directive (more specifically article 33), have led to modifications to this system (see adaptation of the legal framework).

**legal framework**

The statement of conduct is provided on the basis of the Judicial Data and Criminal Records Act (“Wet justitiële en strafvorderlijke gegevens” (Wjsg)). The assessment of applications and the administrative procedure are governed by the Policy Rules VOG 2008 (“Beleidsregels VOG-NP-RP 2008”).

**adaptation of the legal framework**

The Services Act provides in articles 40 to 42 for some adaptations and additions to the legal framework provided by the Judicial Data and Criminal Records Act. These specific articles were needed to implement the obligations defined in article 33 of the Services Directive regarding the exchange of information on criminal records and sanctions within the context of administrative cooperation between the competent authorities of the Member States. The Services Act structures communications on Dutch criminal personal data in accordance with the procedure for exchanging information on the good repute of service providers and via the Internal Market Information system (IMI). Articles 40 to 42 draw on the infrastructure and frameworks offered by the Judicial Data and Criminal Records Act. As a result of this approach, the guarantees offered by this Act in relation to the processing of special personal data will apply. The relevant provisions in this legislative proposal supplement these guarantees and regulate the obligation of a direct and effective information exchange among the competent authorities. Compliance with the principles laid down in the Wbp (Data Protection Act) with regard to criminal personal data is thereby ensured.

Because Article 33(1) of the Directive makes it obligatory to provide information to the competent authority of another Member State, the Services Act deviates from the system of the Judicial Data and Criminal Records Act in which the application for a statement of conduct is made by the service provider. The competent authority of another Member State will have to provide sufficient reasons in accordance with Article 33(1), last sentence, of the Services Directive as to why it is requesting a statement on the service provider in question. The Services Act therefore also opens the way for competent authorities to request a statement next to the already existing possibility for natural and legal persons to do so. The application by a competent authority has to be submitted directly to the Minister of Justice (COVOG). This is in line with the exception provided for in the Judicial Data and Criminal Records Act which allows people who do not have a place of residence in the Netherlands to send a request directly to the Minister of Justice.

The Services Act stipulates explicitly states that the statement of conduct must be applied for by the competent authority via the internal market information system (IMI). IMI has been chosen because it is a quick and easy way for competent authorities to request the statement on the service provider in question. The so-called EloVOG system will subsequently be coupled to the IMI. This system offers

---

the possibility of requesting the statement of conduct entirely by electronic means. This guarantees that the statement can be requested and issued as quickly and efficiently as possible.

The leading idea behind the system of the statement of conduct is that the invasion of the personal life of the parties involved is as proportional as possible. The Judicial Data and Criminal Records Act therefore provides that the application of the statement is made by the party concerned and that the issue or refusal thereof is also made to the party concerned. The party concerned is then of course free to issue the document to, for example, its future employer. In the event that the statement is refused, however, the party concerned can also opt to withdraw from the (application) procedure. However, this is obstructed by the obligation referred to in the Services Directive that the information is issued upon request of the competent authority. That is why it is determined that the intention to refuse to provide the statement is communicated to the service provider concerned. That gives the service provider the opportunity, for example, to withdraw from the authorisation procedure at the foreign competent authority. It is also determined, in accordance with the Directive, that, contrary to the Judicial Data and Criminal Records Act, the application of the statement of conduct is made by the competent authority, after which it is sufficient, with a view to the personal life of the party concerned, to make an announcement that the statement has or has not been provided. The purport of the statement is communicated to the competent authority only in conjunction with the notification of the statement having been issued. The statement or the refusal is then sent to the party concerned so that this party can use the existing objection and appeal options.

In order to prevent a competent authority from being able to request a statement about a party without the knowledge of the person concerned, the EloVOG system is used to ensure that the person concerned gives permission for the application to be dealt with. If the service provider does not give permission, the Minister of Justice must inform the foreign competent authority to this effect as quickly as possible, for then the situation will be that referred to in Article 28(5) of the Services Directive, namely difficulty in meeting a request. It is the responsibility of this body to draw any conclusions regarding the service provider's refusal. The messaging between the Minister of Justice and the competent authorities on the basis of this article will also take place via the IMI system (paragraph 4).

*future plans*

In the course of 2009 steps will be taken to allow employers to request statements of conduct regarding natural persons electronically using the Dutch DigiD-code. The application will in this case be submitted to COVOG directly instead of to the relevant municipality. The required application forms will most probably be filled out using a web form. Specific technical requirements have not yet been determined. A legal basis for the electronic application will most likely be created through an amendment of the Policy Rules VOG 2008.

The statement of conduct itself will still be delivered in a paper format. Currently, there are no pilot projects for making the statement available electronically. However, as follows from the adaptations of the legal framework the purport of the statement is communicated through IMI to the competent authority in conjunction with the notification of the statement having been issued to the natural or legal person.
24.2.3 Extracts from professional registers

document format

Most professional registers are managed by private entities, such as professional organisations, orders or stakeholder bodies. To take stock of the existing possibilities to provide electronic extracts, the following professional registers were examined:

- The register Professions Individual Healthcare (Register “Beroepen Individuele Gezondheidszorg” (BIG-register) of the Healthcare Providers Registration and Information (“Registratie en Informatie Beroepsbeoefenaren in de Zorg” (RIBIZ));
- Roll of lawyers, Amsterdam District Court (“Balie Rechtbank Amsterdam”);
- Royal Netherlands Institute of Registered Accountants (“Koninklijk Nederlands Instituut van Registeraccountants” (NIVRA));
- Netherlands Organisation of Accounting Consultants (“Nederlandse Organisatie van Accountants- Administratieconsulenten” (NOvAA));
- National Institute for Tax- and Companyadvisors (“Nationale Instituut voor Belasting- en Bedrijfsadviseurs” (NIBA)).

None of the above-mentioned registers provide extracts in digital form. Where extracts are made available to the members of a specific profession, this is only done in the form of paper copies. Therefore, it can be assumed that in the Netherlands extracts from professional registers are typically only issued in a paper format. In some cases, paper copies are scanned and sent by email in the form of a PDF-file.

Most organisations that maintain professional registers do offer the possibility to search the register online. Only the BIG-register offers the possibility to apply for registration electronically, using DigID. The decision to allow registration is sent in the form of a PDF-file. However, there is no electronic signature attached to this file.

future plans

To the knowledge of the authors, currently no plans exist to make the use of electronic documents mandatory or to encourage them further.

acceptance by the administration

To the knowledge of the authors, currently there exist no requirements with regard to the acceptance of extracts from professional registers in electronic form in relation to the Dutch administration.
24.2.4 Certificates of insurance

document format
Currently, certificates of insurance are not issued in electronic form.\textsuperscript{500}

future plans
Several steps have been taken to make the issuing in electronic form possible. Firstly, by governmental decree of 8 February 2008 (“Decree”) new provisions were introduced to allow insurers to send announcements regarding insurance contracts electronically.\textsuperscript{501} The insurer may do so, providing that (i) the announcement can be stored on a tangible carrier and (ii) the addressee has given his consent. The announcement is deemed not to have reached the addressee, unless receipt has been confirmed.

Secondly, on 29 February 2008, a proposal was submitted to the House of Representatives to create broader possibilities for drawing up private instruments (“onderhandse akten”) other than in writing.\textsuperscript{502} To these private instruments the conditions mentioned in the Decree apply equally.

In the preliminary opinion of the authors certificates of insurance might fall within the scope of the Decree. However, even if this is not the case, certificates of insurance qualify as private instruments under Dutch law. Consequently, the issuing of certificates of insurance in electronic form will be possible in short term.

To the knowledge of the authors, beyond the information provided above, there exist no requirements with regard to the acceptance of certificates of insurance by the administration.

\textsuperscript{500} The insurance contract is regulated in Book 7, Title 17 of the Dutch Civil Code (“Burgerlijk Wetboek” (BW)). Article 7:933 paragraph 1 BW provides that all announcements based on this title or on the insurance contract are issued in writing. However, according to article 7:933 paragraph 2 BW, deviating provisions may be established which allow for the sending of announcements electronically.

\textsuperscript{501} See governmental decree of 8 February 2008 regarding the sending of announcements by electronic means in the context of insurance contracts (“Besluit van 8 februari 2008, houdende regels inzake de verzending van mededelingen langs elektronische weg in het kader van een verzekeringsovereenkomst”).

\textsuperscript{502} Amendment of certain provisions in the Code of Civil Procedure and the Civil Code in order to allow developments in electronic communication besides the requirement that documents are issued in writing (“Wijziging van enige bepalingen van het Wetboek van Burgerlijke Rechtsvordering en het Burgerlijk Wetboek teneinde naast het in deze bepalingen gestelde vereiste van schriftelijkheid ook ruimte te bieden aan de ontwikkelingen op het gebied van het elektronisch verkeer”).
To the knowledge of the authors, currently there exist no requirements with regard to the acceptance of extracts from certificates of insurance in electronic form in relation to the Dutch administration.

### 24.2.5 Proofs of qualifications

Proofs of qualifications are generally issued by private sector institutions and are only available in paper format. Occasionally, electronic copies are presented in the form of unsigned scans of paper documents. Beyond the general Electronic Signatures Act no specific rules or framework exist for electronic proofs of qualification. To the knowledge of the authors, currently no plans exist to make the use of electronic documents mandatory or to encourage them further.

To the knowledge of the authors, currently there exist no requirements with regard to the acceptance of proofs of qualifications in electronic form in relation to the Dutch administration.

It should be noted that the Netherlands will not apply article 23 of the Services Directive. According to the Services Directive, the transposition and application of this article is optional. The Netherlands have decided not to apply or transpose article 23.

### 24.2.6 Statements from the service provider

It is for the relevant administrations and organisations to determine in specific situations whether service providers will be required to use certain standardised electronic forms and how these will be presented to the service provider. Currently, no mandatory electronic forms exist for general use. However, to support administrations and organisations in their efforts, a project called eForms ("eFormulieren") was started to create a central facility for the development and management of electronic forms in order to reduce administrative costs for the administration, companies and individuals.\(^{503}\)

There are no general guidelines with regard to the form in which electronic statements have to be delivered to the Point(s) of Single Contact by service providers.

requirements in relation to signatures

As has been noted above, administrative authorities may use electronic signatures, providing that the authentication method used is sufficiently reliable, taking into consideration the content and the purpose of the message (article 2:16 Awb). At the moment there are no other requirements in relation to the use of electronic signatures for statements of service providers.

24.3 Delivering electronic documents to services providers in the context of the Point of Single Contact

sending back documents to the service provider

Public administrations and private organisations which fall within the scope of the definition of competent authority of article 1 of the Services Act can choose to deliver messages and documents either through the Secured Message Box, or directly through a connection to their own systems. The service provider can access the message or document through the Secured Message Box and download documents in an open standard format. The functioning of the Secured Message Box is further explained below.

identification of relevant administrations and organisations

The screening of all relevant legislation has resulted in an overview of all administrations and organisations that have to be linked to the Points of Single Contact, and several steps have been taken to support them in their efforts. Firstly, at the initiative of the Ministry of Economic Affairs and the Ministry of the Interior and Kingdom Relations, in September 2007 a report was published on the effects of the Service Directive for decentralized government institutions.504 Furthermore the report on the feasibility of a timely implementation of the Service Directive505 takes stock of the number of administrative authorities, such as municipalities, provinces, water authorities and autonomous administrative authorities that have to take measures in order to comply with the Services Directive. A more detailed list of administrations and organisations has been made by the Working Group on the Implementation of the Services Directive.


To support administrations and organisations in their efforts a guide was published that informs municipalities, provinces and water authorities about the required steps for compliance with the Services Directive. Among other things, this guide contains an overview of the necessary steps for each government organisation in order to connect to the One Counter.

**interaction with the Point of Single Contact**

Service Providers and government bodies will be able to interact through a uniform delivery solution at the national level, namely a Secured Message Box (“Beveiligde Berichtenbox”).

Based on the conclusions put forward in the report on the feasibility of the implementation of the Service Directive (see above p. 5) a pilot version of the Secured Message Box has been developed, that is currently being tested. During the pilot phase, which runs until September 2009, all government institutions will be allowed to connect to the Secured Message Box. During this period the Secured Message Box will only be used for testing virtual accounts and changes to the functionality can still be made. In a later stage new functionalities will be added automatically. After the implementation of the Services Act, connecting to the Secured Message Box will be mandatory under the Services Act.

In short term, the functionalities of the Secured Message Box will be further expanded. The possibility will be created to add folders in which messages can be stored. Also, alternative methods of connecting to the Secured Message Box will be introduced. One alternative method would be to allow government organisations to send messages to services providers from their own ICT-platform by connecting directly to registration systems or document management systems.

The communication through the Secured Message Box goes as follows:

1. The service provider gets access to the Secured Message Box by means of a user name and password. In the pilot version, the service provider initiates the correspondence and determines the character and content thereof. The competent authority can only respond to messages sent by the service provider.
2. The service provider selects the government organisation that he wants to contact.
3. The service provider drafts a message and attaches necessary documents such as application forms.
4. The government organisation receives a notification message.
5. The responsible person logs in to the Secured Message Box.

---

6. The government organisation sends a notification of receipt to the service provider from the Secured Message Box, for example to confirm receipt of an application for a permit. Every email has a time stamp, which indicates the time at which the message was received in the Secured Message Box.

7. After the request by service provider has been handled internally, a response is sent to the service provider through the Secured Message Box.

Informationpoint

Except for a central point of contact for service providers and business recipients, there will also be an Informationpoint (informatiepunt) available for consumers (see Chapter 4 of the Services Act). The Consumer Authority (Article 2.1 of the Consumer Protection Act) is responsible for the Informationpoint. Information mentioned in Chapter 4 will be made available through this electronic Informationpoint for consumers. This information has to be up-to-date, clear, unambiguous and readily accessible. Furthermore, the Consumer Authority supplies the consumer at its request with certain general information on the applicable requirements in the other Member States regarding access to and the performance of service activities. In sofar as is necessary the legal framework applicable to the PSC is mutatis mutandis applicable to the Information Point.

technical and organisational aspects

Currently, the technical and organisational aspects behind the process are handled by the program Answers for Companies (Antwoord voor bedrijven). It is up to the administrations and organisations to designate responsible persons. Possibly, specific rules will be set by ministerial regulation on the basis of article 14 paragraph 1, section a and article 14 paragraph 2 Service Act. Such a ministerial regulation will build on the conclusions that were drawn during the pilot phase.

change to current framework

Until now, no changes to the current framework have been made to regulate the Secured Message Box. However, as has been mentioned above, a ministerial regulation might be introduced.

standards and protocols

The Secured Message Box will make use of SOAP and secured XML.

delivering documents to the service provider

Public administrations and private organizations can choose to deliver documents either through the Secured Message Box, or directly through a connection to their own systems.

changes to the legal framework

Currently, no changes to the legal framework have been announced.
technical requirements

Internal documents with technical specifications. User Guide Secured Message Box has not yet been made public.

status of implementation

See above.

24.4 Assessment – Plans, progress and proposals for further harmonisations

24.4.1 Current plans and progress in the implementation of the Services Directive

At this time, The Netherlands has not identified further issues that need to be addressed at the Community-level. Information on current plans and progress of the implementation of the Services Directive is regularly forwarded to the Commission.

24.4.2 Suggestions for further European support initiatives

At this time, no suggestions are made.
25 Norway

25.1 General framework for electronic documents in eGovernment applications

25.1.1 Electronic documents in eGovernment applications

For a long period of time Norway has had a pro-active approach regarding the regulation of electronic communication, including electronic communication with and within public authorities. This consists of inter alia a large scale project omitting legal impediments for electronic communication (“the eRegulation-project”), secondary regulation to the Administration Act (No. forvaltningsloven) regulating electronic communication and standard regulation on formats on archiving. Before discussing the issues related to the Services Directive and its implementing in Norway, I would like to give a short presentation of these regulatory measures.

In 1999 the Norwegian government established a project ("the eRegulation-project") with the goal to adapt the Norwegian legal system - including all acts, regulations and governmental instructions - to electronic communication and to omit any unnecessary legal impediments for electronic communication in the legal framework. In 2001 the Government proposed a bill to the Parliament, comprising inter alia amendments to 39 different acts, omitting legal impediments for electronic communication. The Parliament passed the bill in December 2001, and the amendments entered into force 1 January 2002.

Secondary regulation on electronic communication with and within the public sector (eGovernment Regulation) from 2004 aims to ensure a secure and effective use of electronic communication with and within the public sector. As a general principle the regulation states that anyone that wants to address an administrative body can use electronic communication, provided it is done in accordance with the form and procedures, and with the use of the electronic address, indicated by the administrative body for that specific request/application.

---

507 Further information in Norwegian concerning this project can be found at http://odin.dep.no/nhd/norsk/tema/VideRe-prosjektet/bn.html
508 Myhr, T., "Kartleggingsprosjektet", Arkivråd, 4/00, s. 17 ff
510 Secondary Regulation of 25th June 2004 no. 988 on electronic communication with and within the public sector (No. forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften))
511 Secondary Regulation of 25th June 2004 no. 988 on electronic communication with and within the public sector (No. forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)) Section 3 (1).
Pursuant to the Act on Records and secondary regulation, there are specific regulations on accepted formats for long term storage of public documents. For text and pictures the following formats are accepted; UTF-8 (for plain text), TIFF, XML and PDF/A. These requirements are realized through a public standard (NOARK). NOARK-4 contains a requirement specification for electronic archives in the public sector, concerning inter alia information content, data structure and functionalities. A new version of NOARK, NOARK-5 version 1.0, was published 4 July 2008 and will replace NOARK-4.

Notwithstanding these regulatory measures, there is not one generic national framework related to electronic documents in eGovernment applications in general. While a relatively large number of eGovernment applications are available to the public, they are to some extent regulated and implemented on an ad hoc basis. But with this on-going shift where electronic communication is replacing paper-based communication, and where it also is possible to file documents with public authorities electronically, one can see an increasing willingness to coordinate and use agreed standards for electronic communication in various public authorities. There are also some reoccurring requirements and formats already used in electronic communication with and within the public sector, which are presented below. As a general comment one can establish that eGovernment services revolve largely around web services.

To better understand the situation in this field in Norway it is also important to have knowledge on the handling of basic data. In Norway there are a few national centralized registers that are used by the public sector and, to some extent, private entities. The two main registers are the National Register and the Central Coordinating Register for Legal Entities.

The National Register holds information about all private persons with some connection to Norway, and who are holding a Norwegian personal registration number. The register is kept by the Directorates of Taxes. The register keeps inter alia information on private persons’ address of residence. It is possible through a web-service solution in All-in, with the use of an electronic signature (for authentication), to register a new address of residence with the National Register.

---

512 Act of 4th December 1992 no. 126 on Archives (No. lov 4. desember 1992 nr. 126 om arkiv (arkivloven))
513 Secondary Regulation of 1st December 1999 no. 1566 on additional technical and record technical requirements on public archives (No. forskrift 1. desember 1999 nr. 1566 om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiv).
514 NOARK = Norwegian Archice Standard (No. Norsk Arkiv standard)
516 It should also be noted that the Government has decided that any governmental public authority that wants to make its services available electronically, has to use the All-in portal (see below) and its extensive infrastructure, or otherwise explain why the All-in solution is not used.
517 Even if the registers are held by one public authorities, other authorities may have an "ownership" to part of the register, and have the right/obligation to make necessary amendments in the register to ensure that it is at all time up to date.
518 All-in (No. Altinn) is a common Internet portal for public reporting. More than 120 forms and services from 20 Norwegian government agencies are currently available through All-in. Since All-in was launched in December 2003 and more than 23 million forms have been submitted through the system. Cf. https://www.altinn.no/en/Toppmeny/About-Altinn/, More About All-in below.
However, the most interesting register in connection to this report is the Central Coordinating Register for Legal Entities. The Brønnøysund Register Centre (hereinafter referred to as “BRC”)\(^{519}\), which is governed by the Ministry of Trade and Industry, consists of several different national computerized registers. The BRC is Norway’s central register authority and source of information. BRC is inter alia responsible for the Central Coordinating Register for Legal Entities (No. Enhetsregisteret). The primary task of the Central Coordinating Register for Legal Entities is to coordinate information on business and industry that resides in various public registers, and which is also frequently requested on questionnaires from the public authorities. Instead of having each public authority send their own separate form for a company to answer, the Central Coordinating Register for Legal Entities ensures that all the information is collected in one place. The Central Coordinating Register for Legal Entities contains basic data about entities that are under reporting obligations to the Register of Employers, the Value Added Tax Registration List, the Register of Business Enterprises, the Business Register of Statistics Norway, the Corporate Taxation Data Register or the County Governors’ Register of Foundations. The Central Coordinating Register for Legal Entities and the Register of Bankruptcies are affiliated registers. All estates in bankruptcy are given an organization number.

The nine-digit organization number identifies an entity, making it easier for the authorities to collaborate on information exchange. Pursuant to the Act relating to the Central Coordinating Register for Legal Entities, other state registers are obliged to cooperate with the Central Coordinating Register for Legal Entities and keep their register information updated.\(^{520}\) As all the various authorities increasingly use a common register for exchanging information among themselves, complying with the form requirements will become easier for all business operators and others engaged in financial activities. Many associations and others with no registration obligation find it useful to register voluntarily with the Central Coordinating Register for Legal Entities. There is no charge for registration. The Central Coordinating Register for Legal Entities only contains information that is stipulated by law, and everyone has access to open register information, such as correct name and address, business objective, industry/branch and representative. Key information can be obtained without cost via the Internet and over the phone. For a fee, printouts from the register can also be obtained with the same information.\(^{521}\)

### 25.1.2 Electronic documents for the purposes of the implementation of the Services Directive

As noted above, any economically active entity in Norway must be registered in the Central Coordinating Register for Legal Entities, and usually also in the Register of Business Enterprises\(^{522}\). The Register of Business Enterprises is responsible for registering all Norwegian and foreign business enterprises in Norway. The register shall ensure the protection of business names against third parties and provide an overview of the financial structure of a business enterprise, and is an important source of information for anyone in need of correct information about participants in Norwegian business and

---

\(^{519}\) Cf. [http://www.brreg.no/english/](http://www.brreg.no/english/)

\(^{520}\) Act of 3 June 1994 no. 15 relating to the Central Coordinating Register for Legal Entities (No. lov 3. juni 1994 nr. 15 om Enhetsregisteret) Section 11

\(^{521}\) Cf. [http://www.brreg.no/english/registers/entities/entities.html](http://www.brreg.no/english/registers/entities/entities.html)

\(^{522}\) No. Foretaksregisteret.
industry. All enterprises operating business activities are obliged to register with the Register of Business Enterprises.

These two registers, the Central Coordinating Register for Legal Entities, and the Register of Business Enterprises, are closely linked to the already mentioned All-in portal (No. Altinn). All-in is a common Internet portal for public reporting, mainly for businesses. The responsibility to administer and develop All-in is allocated to the BRC. In All-in more than 120 different public forms are available and more than 23 million forms have over these past 5 years been submitted through All-in. The amount of compulsory forms submitted electronically has grown significantly since the launch of All-in.

The users of All-in can either fill in the forms directly in the Internet portal or they can use their own IT systems to transfer data, for example salary and accounting systems or a year-end accounting package. The companies' own IT systems transfer pre-filled forms to the portal through a simple interface where subsequently the forms can be completed and signed in the portal.

Efforts have been made to make the forms as easily accessible as possible. The users will automatically get a list of forms on screen when deadlines are imminent and, at the same time, get necessary online guidance on what forms to send to which public agency. All-in automatically enters all relevant information into the forms based on the information already contained in existing public IT systems and registers. The forms are dynamic so there is no need to answer questions that are not specifically related to companies filing the form/information.

All-in is a 24/7 solution and is built on a .NET platform, but in most cases there is no demand for the users to change their hardware or software. Regular access to the Internet is usually sufficient. The solution builds on a standard interface based on an open standard (XML, SOAP), and integration towards the IT systems for the enterprises is implemented through the help of web services. All-in is designed for any security level and the software ensures that access to and treatment of data is restricted to people and software with proper access rights. Security mechanisms are incorporated for secure storage and tracking of data.

In the immediate future several new forms from other government agencies will also be available through All-in. The aim is to provide access to most public forms through the portal. However, Norwegian enterprises are not the sole users of All-in. Several forms designed for private persons are also available through All-in.

To better understand All-in, its capacity and versatility, I would like to present the two following examples of services; the Coordinated Register Notification and filing of annual accounts:

i) The Coordinated Register Notification.

The registration of the incorporation of inter alia private limited companies (No. aksjeselskap), public limited companies (No. allmenjaksjeselskap), partnerships (No. ansvarlig selskap) and individual enterprises (No. enkeltpersonsforetak) can be made wholly electronically through a web-service called Coordinated Register Notification.
The following documents have to be appended; articles of incorporation, minutes from shareholders’ meeting, statement from auditor, company by-laws and relevant agreements. All these documents can be filed in the following formats; Portable Document Format (PDF), Word (.DOC – but not .DOCX), BMP, JPEG, .PNG and .TIFF. All of them are, however, converted to .PDF once received in All-in. No single appendix can be larger than 5 MB, or all together must not exceed 7 MB.

This means that persons incorporating a company can file all necessary information and documents with the Central Coordinating Register for Legal Entities electronically. (It also means that if one document can not be produced electronically this procedure cannot be used and the application with its appendices has to be filled out, signed and filed on paper.) The electronic form will have to be signed electronically by all members of the board, that means several signatures connected to the same registration. In addition the appointed book-keeper and auditor can file “their own documents”, necessary for the registration of the new company, and sign it in the same application.

The application requires that the filed information and documents are duly signed. Those who shall sign must do so personally, this obligation cannot be delegated. The application used in All-in gives information on who is to sign what part of the application. Every signatory receives automatically an electronic document in their All-in “in-box” (accessed by the use of an electronic signature for authentication), which is then to be signed and filed with All-in. Only the designated signatory receives this electronic document, and no one else. The application of registration of the new company is only submitted to All-in when all documents and electronic signatures are in place.

If the signatory of a document is a legal person (e.g. an auditor’s company), the document is sent to the company’s in-box in All-in. The signing can then be duly executed by a person that is registered with All-in as an “administrator” for that company. This role is e.g. automatically granted to the chairman of the board of a company, but can also be delegated.

ii) Filing of annual accounts

Annual accounts shall be filed with the Register of Company Accounts. Annual accounts can be filed in paper-form or electronically. To file its annual accounts the company needs to fill out two forms and to them append inter alia the annual report and the audit report. The form is available as a web-service, and the appendices can be filed in many different formats: doc, dot, rtf, xls, pdf, jpg, gif, png and tiff. (They are all made into pdf-formats once received by the Register of Company Accounts.) In additional several electronic accounting program suppliers have taken use of an interface developed and distributed by the Register of Company Accounts. This enables the companies’ own electronic account programs to transfer pre-filled forms to the portal through this interface where subsequently the forms can be completed and filed.

Thus, it is not surprising that All-in is currently planned to take a central role in the implementing the Services Directive, in the role as a national Point of Single Contact. Subsequently, there will only be one Point of Single Contact in Norway under the Services Directive. All-in is a part of the public administration, administrated by the BRC and subsequently under the Ministry of Trade and Industry. Together with All-in BRC can inform service providers of any requirements for the establishment or for
providing and running their services.\textsuperscript{523} It is clear that their traditional role of assisting service providers corresponds closely to the tasks that the Services Directive foresees for the Points of Single Contact, and also that many services are already available electronically in All-in. From a practical perspective, service providers wishing to become economically active in Norway using electronic means only will need to contact All-in. All-in as a Point of Single Contact will be responsible for ensuring the proper follow-up, including by interacting with any competent administrations or private organizations. The processes to be followed in order to do so will of course depend on the requirements of the specific service provider.

At this time there is no clear detailed plan on how the requirements pursuant to the Services Directive are to be implemented and met under national law. So far, the focus has been to identify the Point of Single Contact (All-in), drafting necessary amendments to existing laws and drafting new regulation. These issues have been sent on public hearing and are now being finalized with the Ministry of Trade and Industry. A proposed bill will be sent to the Parliament early spring in 2009. The government has also been undertaken a screening exercises, to identify which services, applications etc. falls within the scope of the directive and to see whether they already are or can be made available electronically.

It is most likely that the implementation of the Services Directive in Norway is going to be made in several phases. By the end of 2009, the first phase of the implementation will be completed. This will entail implementing necessary legal amendments and to establish All-in as the Point of Single Contact. As already have been mentioned many services and applications are already electronically available through All-in.

As far as the use of electronic signatures and authentication goes, the initial approach is likely to focus on the existing solutions that already exist and are being used in All-in. There are several solutions, on different security levels, accepted in the All-in.

On the highest security level (security level 4) - smart card solution issued by a private company called Buypass\textsuperscript{524}. Security level 3 – pin code from the persons tax reduction card. Security level 2- one-off code from latest tax return, one-off code from a letter ordered by All-in, with a registered password and received one-off code by SMS. Security level 1 – use of a password only.\textsuperscript{525}

In 2009 a new public electronic signature validation authority will be established, and will over time take over the validation services that All-in provides today. This “intercommunication hub”\textsuperscript{526} shall ensure national interoperability between the various electronic signatures issued in Norway, both by private certification service providers and public authorities. There are at this point no explicit plans to open up for the use and validation of foreign electronic signatures.

\textsuperscript{523} Information is today also available through Bedin (www.bedin.no). From 1st January 2009 Bedin will be operated by BRC and their information will be made part of the information given through All-in.

\textsuperscript{524} Cf. www.buypass.no.

\textsuperscript{525} Cf. https://www.altinn.no/ega/Login/Login.aspx?ReturnUrl=%2fega%2facca.aspx

\textsuperscript{526} No. Samtrafikknov.
The government is also planning to issue a citizen card, with an electronic signature on the highest security level (level 4). As of today only private certification service providers issues electronic signatures on the highest security level.

The above-mentioned security levels are mapped to a public standard; “Requirements specification for PKI for the public sector”. This document is a general, functional specification of the requirements applicable to the procurement of PKI (Public Key Infrastructure) for use in connection with electronic communication with and within the public sector. This requirements specification was drafted in response to a resolution adopted by the Norwegian Government requiring a common specification for electronic ID and signature to be formulated by 15 November 2004. The specification forms the basis for common framework agreements for use by the public sector. The requirement specification defines three different electronic signatures; Personal-Standard and Personal-High, both to be issued to physical persons, and Enterprise, issued to legal persons.

The draw-back at this time is that Personal-Standard and Personal-High can only be issued to physical persons holding a Norwegian national identity number. It is this number that is used by the public authorities as the unique identifier. Personal-High is based on a qualified certificate with additional national requirements. The “Enterprise”, however, can be issued also to foreign legal entities. It should also be mentioned that all three types of electronic signatures can be issued by a foreign certification service provider, provided the CSP submit a self-declaration to the National Post and Telecommunication Authority that the requirements are met.

Norway is currently not examining how they can incorporate trusted lists of certification service providers into their solutions, but is working on the establishment of this aforementioned national validation platform. With regard to signature level requirements, while some of the signatures used in electronic communication with the public sector are qualified certificates with additional requirements, it has not yet been decided whether this will also be required of electronic signatures in the cross border context. Before making a final decision in this area, it is most probable that Norwegian administrations first wish to see the direction in which European initiatives are evolving to determine how they can easily integrate an optimal number of electronic signatures from other Member States.

However, in Norway there are limited signature legal requirements, and many public web-services etc. only require authentication for log-on procedures to be able to access their services, and e.g. fill out and submit an electronic form. This fact will probably make it easier to accept electronic signatures as such and maybe also signatures from other EU/EEA-states.

528 No. Post- og teletilsynet.
25.2 Specific document types

25.2.1 Extracts from commercial registers

As already mentioned there are two relevant central registers, the Central Coordinating Register for Legal Entities and the Register of Business Enterprises. Both of them are available, for free, electronically. In the Central Coordinating Register for Legal Entities you can find the following information:

- Business Register Number
- Name
- Organizational form
- Address
- E-mail / url
- Phone numbers
- Date of incorporation / date of registration
- General Manager

BRC also issues extracts from these two registers. Certificates of Incorporation and Register Transcripts can be ordered electronically, but is only issued as a paper document (against a fee). Company Information can also be ordered electronically, and is also issued electronically where you receive an internet link to the ordered information. The electronic information is normally in a pdf-format, and is never signed electronically by the BRC.

Additionally, it is worth noting that BRC participates in the BRITE Project\(^{530}\), which aims at interlinking European business registers, which would eliminate the need for exchanging extracts.

25.2.2 Criminal records

Norway has one central criminal record, containing information on convictions, accepted fines and other decisions concerning inter alia custody/imprisonment, community service and psychiatric care.\(^{531}\) It also holds information on criminal convictions and decisions against companies/legal entities.\(^{532}\)

\(^{530}\) Business Register Interoperability Throughout Europe; see [http://www.briteproject.net/](http://www.briteproject.net/)

\(^{531}\) Act of 11 June 1971 no. 52 on Criminal records (No. Lov 11. juni 1971 nr. 52 om strafferegister) Section 1.

\(^{532}\) Act of 11 June 1971 no. 52 on Criminal records (No. Lov 11. juni 1971 nr. 52 om strafferegister) Section 1, 5\(^{th}\) Paragraph, with reference to the Criminal Code (No. straffeloven) Section 48 a.
To get a criminal record certificate the applicant has to file a written application with the local police authority, stating the legal grounds why he/she needs such a certificate. The Norwegian Police may only issue criminal record certificates when there is a legal basis for it.\textsuperscript{533} It should be noted that such a certificate will not contain information on decisions etc. against a company. Such information is only used in the criminal law administration.\textsuperscript{534}

The application has to be delivered in person, where the applicant has to be able to identify himself by showing an accepted piece of identification; e.g. driver’s license or passport. There are accepted exemptions from the requirement of personal appearance when filing the application, i.a. if you are abroad and cannot fulfill this requirement.

The Application for Criminal Record Certificate is published electronically by the Norwegian Police.\textsuperscript{535} It is published in a pdf-format. The application can be filled out electronically, but it has to be printed out, signed and filed with the local police authority on paper. It is not possible to store the filled out application on the web-page of the Norwegian Police, nor is it possible to file the application electronically to the local police authority.

Normally a criminal record certificate is issued in the Norwegian language, but provided the certificate does not contain any entries of criminal offences, it can be issued in the languages of English, German, French and Spanish.

The police authority, prosecutor authority and courts are entitled to get information from the Criminal offence registry (No. Strafferegisteret) concerning specific individuals. Such information is provided on a specific form, i.e. on a paper copy.\textsuperscript{536}

To my knowledge there is no ongoing work in this field, making it possible to apply for or receive a criminal record certificate electronically.

\subsection*{25.2.3 Extracts from professional registers}

\textsuperscript{533} Pursuant to Secondary regulation of 20 December 1974 no. 4 on criminal offences registration (No. forskrift 20. desember 1974 nr. 4 om strafferegistrering) it should be noted that all persons have a right of access to the information in his/her criminal record. This is usually done by personal appearance at the local police authority, where the information is given orally.

\textsuperscript{534} Act of 11 June 1971 no. 52 on Criminal records (No. Lov 11. juni 1971 nr. 52 om strafferegister) Section 6.

\textsuperscript{535} cf. \url{http://www.politi.no/pls/idesk/docs/f1197274794/gp-5168-e.pdf}.

\textsuperscript{536} Cf. Secondary regulation of 20 December 1974 no. 4 on criminal offences registration (No. forskrift 20. desember 1974 nr. 4 om strafferegistrering) Section 6, 1st paragraph
While it is difficult to obtain a complete overview, it appears that extracts from professional registers are commonly issued in a paper form. There are, however, no apparent legal obstacles that would prevent issuers of these extracts to issue them in an electronic form. Eg. the Supervisory Council of Legal Practice only issues paper based certificates stating that a person hold the title as an attorney-at-law under Norwegian law. The Council has on the other hand a database with the information on who holds the title attorney-at-law, and courts and other public authorities that need such information have access to this database.

In the process of registration a new company the BRC only to limited extent verifies if the necessary authorizations or approvals are in place. In many cases a self-declaration is enough, e.g. when incorporating a law-firm it is enough for the founders and owners to submit a self-declaration that they are attorneys-at-law. On the other hand, companies that need an approval from the Financial Supervisory Authority have to submit this approval to the BRC. The copy of the approval shall be sent to the BRC. If the registration is done electronically the approval is scanned (in pdf-format) and sent together with the Coordinated Register Notification, where the whole application with its documents is signed electronically. The approval is thus not electronically signed by the Financial Supervisory Authority to ensure its integrity. According to the BRC this has nevertheless never been a problem. This means that there is a limited, or even no, need to have electronic issued extracts from professional registers.

It can be mentioned that there is an application where medical doctors can send electronic documents (using XML-format) to the Norwegian Labor and Welfare Organization. With the use of an ebXML framework and PKI (delivered by a private company – Zebsign) medical doctors can electronically send in certain types of documents using this electronic signature that also verifies that the signer is a medical doctor.

### 25.2.4 Certificates of insurance

There are no legal obstacles under Norwegian law for insurance companies to issue certificates of insurance electronically. But to my knowledge certificates of insurance is not produced in electronic form to a large extent. If they are issued electronically they usually are issued in a pdf-format, unsigned. To what extent these certificates are being used has not been possible to establish, but probably to a very small extent. Any legal rights and obligations under an insurance policy are normally established with the direct involvement of the insurance company, where there is a limited need for an electronic certificate of insurance.

### 25.2.5 Proofs of qualifications

537 (In 2009 a new national validation authority will be established, and will over time take over the validation services that All-in offers today. This "intercommunication hub" shall ensure national interoperability between the various electronic signatures issued in Norway, both by private certification service providers and public authorities.)

538 Cf. www.zebsign.no.
The same comments made above in relation to extracts from professional registers apply also to proofs of qualifications: generally, these documents are only available as paper originals. While electronic copies might occasionally be presented in the form of unsigned scans, this is merely a matter of convenience. No specific rules or framework exist for electronic proofs of qualification, and no plans have been proposed to encourage or mandate their uptake.

### 25.2.6 Statements from the service provider

Statements made by the service provider himself when eg. incorporating a company can usually be integrated into the websites of the Coordinated Registration Notification as web forms to be completed and signed. This is already a functioning application where appended pdf-files are electronically signed together with the main form.

Pursuant to the Public Procurement Act\(^\text{539}\), suppliers always have to append certain documents to their offers; inter alia tax certificate and EHS\(^\text{540}\) statement. To simplify the process of delivering offers for the suppliers, there is an ongoing project where these standard documents can be filed with a national suppliers register, and it is enough for the suppliers to inform that they are available there. This is a project still in its cradle, and thus it is not decided who will be in charge of such a register, how documents can be filed and who can access them and how. This again shows that the Norwegian approach is not to issue electronic documents, but with the aim of reducing administrative burdens instead establish a centralized register holding relevant information and ensuring those in need of that information to have proper access to the registered information.

### 25.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

#### 25.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As was noted above in the explanation of the tasks of BRC and the All-in portal, the identification of the competent public administrations and the interaction with them is already one of their core functions. This will thus remain the same after the implementation of the Services Directive. All-in, acting as a Point of Single Contact, will be in charge of identifying the appropriate bodies that need to be communicated with on behalf of the service provider. The link between All-in and other public bodies/agencies are already in place, and hence the main change will be the increased number of services and public bodies that All-in will have to interact with due to the implementation of the Services Directive. After having discussed the implementation of the Services Directive with the responsible persons with the Ministry of Trade of Industry, I have been informed that to their knowledge at this present stage there are no wholly private organizations that All-in, acting as a Point

\(^{539}\) Act of 16 July 1999 no. 69 on Public Procurement (No. Lov 16. juli 1999 nr. 69 om offentlige anskaffelser)

\(^{540}\) EHS = environment, health and security (No. HMS-erklæring)
of Single Contact, will have to interact with. This also includes professional registers, which are public entities under Norwegian law. It has to be made clear that the government at this present state does not have a complete picture of all parties the Point of Single Contact will have to interact with. This will be an issue that will have to be addressed in connection with the establishment of All-in as a Point of Single Contact.

It is not clear how All-in, also with the use of the coming national validation authority enabling interoperability on a national level, shall validate foreign electronic documentation that service providers of other Member States relies on.

As noted above, while the All-in portal has already been in operation for quite some time. It will not provide all the services described above until the required legislative amendments have entered into force.

25.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Communication with All-in and service providers can be made electronically. Substantial information on how to start and run a business can be found on the web-pages of All-in. In addition, as already been mentioned, many forms and applications can be filled out and filed electronically, normally by the use of web-services. It is also possible to sign these electronic forms, but with some mentioned limitation for foreigners that are not holders of, or cannot be holders of, a Norwegian personal identification number. Enterprise certificates are not yet used in the All-in portal.

All-in and BRC has an open telephone line – support - where users of their services can get answers related to the different forms available through the All-in portal, and also technical support on the use of electronic forms and electronic signatures. All-in and BRC has also an e-mail address to which their users can send their questions.541

541 https://www.altinn.no/no/Toppmeny/Kontakt-og-hjelp/
25.4 Assessment – Plans, progress and proposals for further harmonisation

25.4.1 Current plans and progress in the implementation of the Services Directive

As shown in the overview above, Norway already has an advanced infrastructure in place that can be leveraged for the implementation of the Services Directive, in the form of the All-in portal that already supports part of the functions expected of the PSC; and in the form of the Central Coordinating Register of Legal Entities which acts as an official register of essential information related to service providers. It is thus not surprising that it is planned to leverage this infrastructure to a significant degree in implementing the Directive.

With regard to electronic documents, Norwegian experience is limited but that is to a large extent due to the fact that electronic documents are not needed since there is a functioning system of sharing of information from databases in place in many areas. As noted above there are several central registers that are accessible on-line or through downloading once every day (batch) to other public administrations, which significantly limits the need for electronic documents.

This does not necessarily mean that electronic documents would be entirely unused by the Norwegian Point of Single Contact, but rather that they would not become a key part of the Norwegian strategy to implement the Services Directive. If this would turn out to be necessary, it would be feasible to create electronic documents containing the registered information using any number of common standards. As already noted above, Norwegian administrations have relied on various formats – but mainly on pdf-formats - to produce electronically signed documents, and this would be a possibility for the implementation of the Services Directive as well, if there would be a need to do this. However, generally speaking, the Norwegian approach much favors the elimination of documents (paper based and electronically) and relying on the creation of trusted networks of authentic information instead, which can be accessed by duly mandated parties through specific web services. Such a solution will require that necessary privacy issues are duly addressed. As the aforementioned example of BRITE shows, this is a model that could also be applied in a cross border context.

25.4.2 Suggestions for further European support initiatives

Given the Norwegian emphasis on authentic sources and web services rather than electronic documents, the creation and expansion of trusted networks to exchange authentic information between mandated parties would seem to be a favored option. However, as an interim step, Norway would also welcome further harmonization of existing electronic documents. From a technical perspective, the Norwegian infrastructure would be able to accommodate most widespread standards, so that there is no specific preference in this regard. Similarly, if this would be necessary and beneficial, it would be possible for Norwegian administrations to deliver electronic documents as well via web services. This would, however, require changes of today’s organization and structure of electronic communication.
With regard to electronic signatures, there is a more problematic issue. There are already functioning solutions for electronic signatures and they will be improved with a centralized national validation authority – enabling national interoperability of electronic signatures – and the issuance of a National Citizen Card with an electronic signature. But the problem is the validation and acceptance of foreign electronic signatures and/or the issuance of national personal electronic signatures to foreigners that do not have a Norwegian personal identification number. Norway would probably favor the establishment of a cross-border validation authority solution, rather than having a cross-national validation where national authorities are supposed to validate any electronic signature issued within the EU/EEA on a certain security level.

At any rate, key difficulties in practice include the determination of the reliability and responsibilities of service providers of other Member States. However, given the fact that already electronic signatures issued by private certification service providers are accepted in electronic communication with public authorities in Norway, the mere fact that a foreign electronic signature is issued by a private certification service provider will not as such be problematic or politically sensitive, especially if the certification service provider in question falls under a national supervisory scheme. The issue of cross-border interoperability is a problematic issue and is certainly a field where European initiatives could be useful in order to improve trust or facilitate validation of electronic signatures.
26 Poland

26.1 General framework for electronic documents in eGovernment applications

26.1.1 Electronic documents in eGovernment applications

Poland has established a general legal framework for eGovernment in the Act on Informatisation of Activities Undertaken by Entities Fulfilling Public Tasks. Most relevantly for this study, Art. 16 (1) thereof requires that public bodies enable “communication by means of electronic documents” as a part of the government service delivery process. The same act defines “electronic document” as “a complete set of data making up a separate meaning, arranged in a defined internal structure and recorded on an informatic data carrier” (Art. 3(2)).

Further requirements for electronic documents in eGovernment are statutorily refined separately for documents delivered (1) to public bodies and (2) by public bodies. These two groups are briefly discussed in turn.

Ad (1) Technical requirements regarding electronic documents delivered to public bodies are laid down in the Ordinance of the President of the Council of Ministers on organisational and technical conditions for submitting electronic documents to public bodies. The Ordinance covers Polish public bodies, authorities from other EU Member States and EU citizens, when they submit an electronic document to a Polish public body. On the other hand, it leaves outside its remit documents sent by a public body to entities not recognized as “public bodies” by the Act, e.g. public authorities of other EU Member States or EU citizens.

The Ordinance requires that electronic documents be delivered to public bodies in formats prescribed by another executive act: the Ordinance of the Council of Ministers on minimal requirements for teleinformation systems. The latter Act establishes formats and protocols supported by eGovernment applications. As the most relevant example, each eGovernment application enabling transfer of documents should be compliant with at least one of the following formats: .txt, rtf v. 1.6, .pdf v. 1.4, .doc, Open Document v. 1.0. Moreover, the Ordinance on organisational and technical conditions for submitting electronic documents to public bodies requires that the entities define the structure (forms) of documents accepted (§ 4), though imminent consequences of ignoring the

542 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2005 Nr 64 Poz. 565, with further amendments.
543 Rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym, Dz. U. 2005 Nr 200 Poz. 1651.
544 Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych, Dz. U. 2005 Nr 212 Poz.1766.
obligation remain unclear. Furthermore, each public body is obliged to establish an electronic contact point (elektroniczna skrzynka podawcza) for electronic submissions (§ 5(1)). Contact point details, including their on-line addresses and submission requirements, should be published on an official web-page of each public body (§ 5(2)). Additionally, when initiating the administrative procedure with an electronic document, the applicant must, according to Art. 63 § 3a Administrative Procedure Code,

(1) sign the application with a secure electronic signature verified with a qualified certificate and (2) submit it only in the form prescribed, if so required by law. Statutory provisions in almost every area undergoing informatization require separate executive acts to prescribe the structure of documents used in detail. Legal stability is enhanced in effect, at the expense of flexibility, however, and the feasibility of improving the system if the requirements devised in advance turn out sub-optimal after the implementation.

Conditions of making electronic forms available to recipients of certification services (users of electronic signatures requiring third party certification) are further regulated by the Ordinance of the Minister of the Interior and Administration of 24 July 2007 on conditions of making available forms and templates of documents in electronic form. Despite the fact that the Ordinance explicitly refers only to forms used by a certain group of users (it does not deal with all the recipients of eGovernment services explicitly), in practice its effects are overarching, predominantly due to the growing body of legal provisions, which, like the abovementioned requirement of the Administration Procedure Code, require electronic signatures associated with a qualified certificate. The Ordinance provides that templates of electronic forms used by recipients of certification services be transmitted to a central repository maintained by the Minister of Interior and Administration and published therein (§ 3(1), § 4). Information on availability of the forms, and availability of the forms themselves, should be revealed by public authorities on their web-sites (§ 3(2), § 6(2)). Each template should be generated in XML and described in an XML Schema (XSD) (§ 3(3)). The Minister of Interior and Administration is obliged to publish the XSD Schema on the official web-site of the Ministry (§ 3(4)).

Ad (2) Legal and technical requirements for electronic documents delivered by public authorities to subjects of the administrative procedure are comparably complex. The relevant Ordinance of the Minister of the Interior and Administration of 27 November 2006 on creating and delivering electronic documents requires that the documents be compliant with the abovementioned minimal requirements for teleinformation systems (§ 3(1)) and signed with a time-stamped secure electronic signature compliant with the XML Advanced Electronic Signatures (XAdES) standard ETSI TS 101 903 V1.3.2 or newer (§ 3(2)). Similarly to the abovementioned requirements for electronic documents accepted by public bodies, forms of documents discussed now should be passed to the central repository maintained by the Minister of the Interior and Administration, and published therein (§ 3(4),

545 Ustawa z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, Dz. U. z 2000 r. Nr 98 Poz. 1071 (cons. text), with further amendments.
546 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2007 r. w sprawie warunków udostępniania formularzy i wzorów dokumentów w postaci elektronicznej, Dz. U. 2007 Nr 151 Poz. 1078.
547 The repository was launched in mid-2007 at www.crd.mswia.gov.pl, and moved to http://epuap.gov.pl afterwards. At the end of November 2008 it contains only a minuscule number of 21 templates.
548 The schema is available at http://www2.mswia.gov.pl/portal/pl/2/4757/.
549 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 listopada 2006 r. w sprawie sporządzania i doręczania pism w formie dokumentów elektronicznych, Dz. U. 2006 Nr 227 Poz. 1664.
§ 3(5)). Additionally, the forms should be made available by relevant public authorities on their websites (§ 3(5)), despite the fact that the forms are of limited usefulness for recipients of eGovernment services.550

Regarding another important issue of the Ordinance - the document delivery procedure – it is particularly worth mentioning that the document authorization process requires in each case that the recipients sign a receipt with a secure electronic signature verified with a qualified certificate (§ 4(3)).

As an issue indirectly related to electronic documents as such, but crucial for their delivery, the Ordinance requires that (for sending access codes, documents and receipts) public authorities should use secure channels based on one of the two relevant minimal requirements for teleinformation systems of electronic documents (either SSL v. 3/TLS or S/MIME v. 3) or the https protocol (§ 4(7)). Also, the authorities must record data necessary for establishing when the document is sent by the public authority and received by the recipient (ld'). Moreover, the system ought to allow for marking the documents with data establishing validity of the relevant electronic certificates and the certification time. To this end, the system must be compliant with the ETSI norm CEN-CWA 14167-1 (March 2003 or newer), must use the HSM cryptographic module compliant with the norm FIPS 140-2 level 3 or CEN-CWA 14167-2 or newer, must employ appliances adjusted to the official coordinated time UTC(PL), and must use cryptographic algorithms of at least 2040 bits long (§ 4(8)).


In order to limit communication costs incurred by public authorities and to enhance coordinated operability, the Ministry of the Interior and Administration is developing one of the main ICT projects currently implemented in Poland – the Platform of Public Administration Services (Platforma Usług Administracji Publicznej, hereinafter: e-PUAP) – http://epuap.gov.pl/wps/portal/epuap. The platform serves as a common non-physical infrastructure for eGovernment applications. It is to provide public authorities with a growing body of services required by law, at technical standards compliant with statutory requirements (as to the date of submitting this report virtually all of the public authorities obliged to accept electronic documents have had a mail-box compliant with legal requirements set up at the e-PUAP).

---

550 If heeded that the group currently discussed regards electronic documents produced by public authorities, not those submitted by their customers.

551 Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych, Dz. U. 2006 Nr 206 Poz. 1517.
26.1.2 Electronic documents for the purposes of the implementation of the Services Directive

The implementation of Art. 8 Services Directive will be undertaken in Poland pursuant to the amendment to the Act of 2 July 2004 on Freedom of Business Activity (hereinafter: FBA). At the date of submitting this report, the draft amendment act has been almost unanimously accepted by the lower chamber (Sejm) of the Parliament (on 21 November 2008). No significant alterations are expected in the higher chamber (Senate), so the relevant amendments will be invoked below as if they were a part of the formal legislative text already.

As a fully-functional model of the PSC (provided by the FBA) will be implemented in Poland from July 2011 only, a brief description of the transitional model and registration issues outside the ambit of the FBA is warranted first.

Currently an entrepreneur may, when applying for the Register of Business Activity (Ewidencja Dzialalnosci Gospodarczej), submit notifications to other relevant authorities (art. 7b Act of 19 November 1999 Law of the Business Activities). In this scenario notifications/applications for other authorities are transmitted thereto by the local commune (Gmina) authority, pursuant to back-office management processes. Theoretically the application and notifications could be submitted electronically, pursuant to the general legal arrangements discussed in the previous section of this report. At least at the moment, however, neither the electronic front-office channel of communication, nor even the paper single point of registration is used in practice. This is predominantly because IT systems of the relevant authorities are not interoperable, and thus the whole procedure requires paper back-office mailing, causing delays. Service providers therefore prefer completing the procedure in person.

From April 2009 the SPA procedure will be made obligatory. Local commune authorities will transfer notifications/applications to statistical, tax and social security authorities, both on paper and electronically (Art. 45 (1) FBA). Details on how registration applications and accompanying documents will be transferred shall be established in an ordinance of the Minister of Economy. The ordinance is to take extant “capabilities of electronic processing of data and the content of the data” into account (Art. 45(4) FBA). While the transfer should be undertaken “without delay”, it is still to be seen whether the procedure will ensure convenience, or rather cause delays instead. First, as above-mentioned, the current paper procedure will not be replaced but only supplemented with the electronic one, thus it will not eliminate the main inconvenience of the current system. Second, the Ministry of Economy, questioned about an outline of the back-office procedure details four months before the legislative deadline could not provide any substantially relevant information, even on a blueprint of the executive ordinance.

552 Ustawa z dnia 2 lipca 2004 r. o swobodzie dzialalnosci gospodarczej, Dz.U. 2004 Nr 173 Poz. 1807, with further amendments.
553 Ustawa z dnia 19 listopada 1999 r. Prawo dzialalnosci gospodarczej Dz.U. 1999 nr 101 poz. 1178, with further amendments. Essentially the same procedure will be maintained after the provision is replaced by Art. 44 FBA from April 2009.
The procedure is irrelevant for the registration to the National Judiciary Register (Krajowy Rejestr Sądowy), a separate register for bigger, corporate companies. In fact amendments provided by the FBA in this respect, and entering into force from April 2009, are discordant with Art. 8 of the Services Directive. An amendment to Art. 19b(1) Act on the National Judiciary Register provides that applying for the registration into the National Judiciary Register would automatically amount to notification/application for statistical, tax and social security purposes. The registration court would transfer the information to relevant authorities. However, the amendment mentions no electronic back-office procedure in this respect (even one merely collateral to paper). Moreover, it explicitly excludes the SPA procedure when the registration application is submitted in the electronic form (Art. 19b(1c)(1) Act on the National Judiciary Register). In the latter situation the applicant herself is obliged to fulfill the remaining notification obligations. Presumably the same procedure will stand after July 2011, as the National Judiciary Register is entirely independent from the Register of Business Activity or its institutional successors.

From July 2011 the current, dispersed and non-interoperable mesh Register of Business Activity maintained by each of about 2500 local communes will be replaced by a central database - Central Register and Information on Business Activity (Centralna Ewidencja i Informacja o Działalności Gospodarczej – hereinafter: “CEIDG” or “System”). The CEIDG will automatically exchange data with other public systems so that the entrepreneur will be able to complete all the registration formalities by interacting with the CEIDG only. Back-office procedures will employ an electronic channel only, safeguarding fast completion of the registration/notification procedures (Art. 24(5-6), 28 FBA).

The CEIDG shall be maintained by the Minister of Economy, with a fourfold purpose (Art. 23(3) FBA):

1) inventorying business activities by individuals;
2) making unrestricted information publicly available on the Internet;
3) making available the registration data on entrepreneurs entered into the National Judiciary Register;
4) allowing for determining dates and ranges of alterations into the System, together with identities of users inserting them into the system.

The CEIDG will be restricted to a database storing registration information. Data transmission between the Register and users will be enabled and mediated by the ePUAP platform (Art. 24(1) FBA). Electronic forms allowing for introducing information into the database will be available through the main web-page of the CEIDG, through the official web-page of the relevant Minister, and through the ePUAP (Art. 24(2) FBA). The template of forms used is to be defined by an Ordinance of the Council of Ministers (Art. 25(6) FBA).

The FBA provides for a two-track procedure of entering registration data to the CEIDG: either by the entrepreneur herself or through a local commune authority, according to the choice of the entrepreneur.

554 Ustawa z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym, Dz.U. 1997, Nr 121, Poz. 769, ze zm.
555 Through its on-line interface available at http://pdi.cors.gov.pl/KRSSED/ the system of the National Judiciary Register allows for searches according to registration numbers or names of registered companies. The system reveals registration numbers, statistical numbers, names, addresses, dates of registration and deletion from the registry, and representation details of the sought company.
In order to complete the registration procedure in person, the entrepreneur will fill out an on-line form (Art. 26(1) FBA) and sign it with a secure electronic signature verified with a qualified certificate (Art. 27(7) FBA). If the form has been filled out incorrectly, the system will not accept it, and the applicant will be informed electronically about the grounds (Art. 27(3) FBA). Other identification registers will be used to cross-verify the data submitted (Art. 27(5) FBA). The application will be free of costs (Art. 29 FBA).

As an alternative, the entrepreneur can submit the registration application form to any of the local community authorities on paper, either in person or using registered mail (Art. 26(2) FBA). An authorised office-worker will verify information submitted in the application and insert the data into the System (Art. 26(3-4) FBA).

The CEIDG will make the registration information available on-line, except for sensitive data regarding individual entrepreneurs. In other words, the available information will comprise of the company name, statistical and tax number (if assigned), citizenship of the entrepreneur, company address, company e-mail and web-page if held, date of establishment, official classification number of the company activities, information on civil law partnerships, joint property of husband and wife, data on attorneys appointed, information on suspension or resuming of business activities, restrictions in the legal actions capacity, information on bankruptcy or reorganisation proceedings, information on bans on economic activities (Art. 25(1) FBA).

Additionally, the CEIDG will reveal information on concessions, licenses, permissions or inserts into registers of regulated activities (Art. 37(2) FBA). The FBA provides that the information will be passed to the CEIDG (Art. 37(5)). The Ministry of Economy did not confirm that this provision should be interpreted as requiring that source authorities insert the information into the System directly. If that is the case, it is still to be seen to what extent the communication platform of ePUAP will manage this function. It is apparent, however, that the issue has been clearly underestimated, by the Ministry of Economy at least.

Information from the CEIDG will be made available on-line, through the ePUAP (Art. 38(1-2) FBA). An executive Ordinance may determine languages in which registration information will be presented by the CEIDG, “taking into account the necessity of international cooperation and enhancing security of international trade” (Art. 38(3)). The information will be available on-line up to six months after deletion of the registration entry. Afterwards it will be archived and revealed only pursuant to a written application, except for the name and the date of deletion, which presumably still will be available on-

556 In the latter situation the signature should be authenticated by a notary (Art. 27(9)).

557 I.e. the official personal identification number – PESEL – as it allows for deciphering the birth date, and the address of residence if different from the company address (Art. 37(1)(1) FBA).

558 The statement of grounds of the legislative proposal (p. 9) explains that revealing this information is important for potential business partners, because it allows them do determine legal culture of the entrepreneur and the language which should be used in marketing information.

559 No user account will be required in the CEIDG system to browse through registration information. It has not been determined, however, if one would need to set up an account on the ePUAP in order to use it for these purposes.
Public authorities might receive a “wholesale” access to the registration information for free after settling technical conditions with the Minister of Economy (Art. 39(1) FBA). The “wholesale” access may be obtained by other entities (commercial and non-commercial purposes alike) also, for a fee and on a basis of a contract signed with the Minister of Economy, if the entity seeking the access additionally possesses measures (1) necessary to identify persons accessing the data, scope, date and purpose of the access, (2) preventing from illegal use of the data (Art. 39(2-4) FBA). Further trade of data is foreclosed, unless otherwise stipulated in the contract with the Minister (Art. 39(5) FBA).

As an issue particularly important for this report, extracts (certificates) from the CEIDG will be maintained, in the electronic form or as printouts from the System (Art. 38(4) FBA). On the other hand, however, public authorities will not be allowed to request certificates from the entrepreneurs (Art. 38(5) FBA), arguably because they can consult the source information in the CEIDG system directly. Institution of certificates will therefore aim essentially at preserving solemnity of the document, no matter how impractical it might be considering the new institutional circumstances. As a consequence, the FBA authorizes the Minister of Economy to issue an Ordinance stipulating how the certificates (both in the electronic and paper form) should be created, transferred and protected, “taking into account trade security, protection of company interests and security of data transmission” (Art. 38(6) FBA).

26.2 Specific document types

26.2.1 Extracts from commercial registers

It is worth to recapitulate that there are two commercial registers in Poland: the National Judiciary Register (corporate enterprises) and the Register of Business Activity (entrepreneurs).

Formal extracts from the National Judiciary Register are available in the electronic form. To receive them, applicants are to sign their requests with secure electronic signatures verified with a qualified certificate and pay the fee. This procedure requires human processing. On the other hand, as mentioned earlier, a broad range of registration information is freely searchable through the Registry website. It is thus unsurprising that only the second option is used in practice, making the question of official electronic extracts from the register devoid of practical significance.

Many local nodes of the Register of Business Activity are searchable on-line, but no extracts from the Register are available in the electronic form. It is predictable that electronic extracts will not play significant role after July 2011, either (when the institution of electronic certificates will be introduced), as the same information will be fully available on-line and public authorities will not be authorised to

560 By comparison, deletion from the National Judiciary Register (or elapse of time thereafter) does not influence availability of the information through the internet search.

562 See supra, ft. 14.
request the extracts. This trend is appreciable, as there is no significant reason to migrate the certificates (and requirements to present them) into the digital environment.

26.2.2 Criminal records

Extracts from the penal register (also known as no-conviction certificates - zaświadczenia o niekaralności) are issued in the paper form only. Moreover, applications may be submitted only in the same form, either in person or by post. Forms are downloadable from the web-page of the Ministry of Justice (http://www.ms.gov.pl/krk/krk.php) and should bear appropriate fee stamps. The latter requirement makes migration of the criminal records into the digital form virtually impossible.

26.2.3 Extracts from professional registers

No digital extracts from professional registers are issued in Poland. Essentially, there seems to be no potential demand for them, as the extracts are either needed for proffering during an inspection or to be placed in the location of the vocational activity. Digital extracts are poorly positioned to fulfill these functions (except for the on-line environment where, however, using them is neither required nor needed).

As professional registers are normally maintained in the digital form in Poland, the more important issue is that of access to register information on-line. In the context of the CEIDG 563 this implies a choice of whether this register should be fully interoperable with professional registers or manually fed with information produced therein. The second option is expected to be implemented in Poland from July 2011. It eliminates up-front costs of providing interoperability, being less efficient and thus more expensive in operation at the same time.

26.2.4 Certificates of insurance

Electronic certificates of insurance are legally permissible under the terms of the Act on Electronic Signature. 564 Certificate recipients do not use them, however, in on-line relations (which is the proper and the most natural environment of their use) and thus the usefulness of a form other than paper remains theoretical only.

---

563 The nature of enterprises entered into the National Judiciary Register makes it irrelevant for this discussion.

564 Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym, Dz. U. 2001, Nr 130, Poz. 1450, with further amendments.
26.2.5 Proofs of qualifications

Proofs of qualifications are required in traditional, off-line situations only. Thus the potential for digital technologies seems to rest in the sphere of the ubiquitous and instant availability of original authoritative information certifying qualifications on-line (with no requirement to produce separate proofs or other documents), rather than in substituting one format (paper) with another (digital), with the basic mechanism of requesting the document intact.

26.2.6 Statements from the service provider

Theoretically, statements from service providers could be produced and delivered in the electronic form, either as a plain e-mail, or, for more solemn statements, signed with a secure electronic signature verified with a qualified certificate (or some other authentication mechanism acceptable and convenient for both sides). Yet, no electronic statements function in eGovernment relations.

26.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

26.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

In the fully-fledged version (from July 2011) of the PCS, the back-office communication between public authorities responsible for distribution of documents relating to access to a service activity is planned to be enabled through the ePUAP platform. The platform will provide all the requisite communications tools (including user identification, data transfer authorisation and validation). This features highlight the role of the platform as a „registration broker,” an overlay on key governmental information resources. Coordination services provided by the ePUAP should allow for producing more complex services, combining information resources into a new product. As an upshot, back-office services will rely on both the CEIDG and the ePUAP inseparably.

In the intermediary model (from April 2009 to July 2011) the back-office transfer of documents will be undertaken in both paper and electronic form.

No further technical details have been decided so far, however.
26.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

In the mature model, i.e. from July 2011, the communication between the PSC and the service provider will be mediated by the ePUAP. To this end the service provider will use a web-application to submit a threefold (CEIDG, tax and social security purposes) form of notifications on-line and will be required to use secure electronic signature verified with a qualified certificate to sign the data package uploaded. As an alternative, the entrepreneur will visit a local commune public authority to submit the paper form, or will send it with a registered mail (signature authenticated by a notary). The optional paper procedure aims at avoiding discrimination of digital have-nots, those entrepreneurs who are not technically prepared for electronic transactions. It is predicted that the digital gap should be closed in five years following July 2011, and that the paper procedure option will withdrawn when the demand for it expires.

The transitional model (up to July 2011) will rely on the paper form of the front-office.

26.4 Assessment – Plans, progress and proposals for further harmonisation

26.4.1 Current plans and progress in the implementation of the Services Directive

The implementation of Art. 8 Services Directive will depend predominantly on the development of appropriate technical and organizational infrastructure necessary for unifying the dispersed system of the Register of Business Activity and interconnecting it with other public systems through the ePUAP. To that end, the ePUAP platform is being constantly improved. Its interoperability with the tax and social security systems is currently under tests in one of the Polish regions (a project called "Wrota Podlasia"). Thus it is rather certain that the interoperability platform will be fully functional before 2011. The two and a half year period is required rather for developing the CEIDG itself and an authentication platform based on the concept of electronic ID (pl.ID). Among less encouraging traits three are worth mentioning. First, in November 2008 the Ministry of Economy is not able to provide any information on how the back-office PSC electronic procedure will look like from April 2009. Second, no electronic PSC procedure is planned for registrations to the National Judiciary Register, either before or after 2011. Third, the procedure of drafting a feasibility study for the CEIDG has not even been started yet and it is not quite clear how this would be coordinated with drafting necessary executive measures to the FBA.

The issue of eGovernment documents, on the other hand, seems of secondary importance, as the legislative arrangements focus on making source registration information available on-line, maintaining registration certificates rather for symbolic purposes, and using web-application for submitting registration information, instead. This trend is appreciable as allowing to reduce costs of circulating copies of documents, and as enhancing reliability of the official information at the same time. Also, because Internet penetration grows rapidly in the group of users covered by this report (entrepreneurs, public authorities), the problem of the digital divide should not be considered as an impediment to the approach chosen.
More problematic is the demand for the planned solutions among users. Even if the main reason for the rejection of the currently available one-stop-shopping (paper) procedure is the delays caused by the paper back-office processes, a limited take-up of secure electronic signatures verified with qualified certificates, heavily promoted in all eGovernment applications, makes it uncertain whether relations based on the same type of authentication will succeed in the front-office PSC relations. It is worth mentioning in this context that gradually since July 2008 bigger enterprises have been forced to use this type of signatures in social security relations. It is uncertain, however, how this will impact the take-up of the electronic front-office CEIDG registration procedure from July 2011. Conjecturally, the impact may be very limited, considering that the registration is the first act of establishment (i.e. it occurs before the social security related obligations of using electronic signatures are triggered) and the obligation to use electronic documents does not apply to enterprises that pay social security contributions for no more than five persons.

Thus the obligation to use the signatures for social security purposes regards in the first place bigger, corporate enterprises, entered to the National Judiciary Register. Entrepreneurs submitting their applications for registration to the CEIDG may be rather willing to avoid the up-front costs of procuring tools and services indispensable for using secure electronic signatures verified with a qualified certificate. Plans to introduce the pl.ID may change the calculations to some extent (depending on how much of the current costs of using electronic signatures the new ID will eliminate). It is too early to predict on the latter issue, however.

26.4.2 Suggestions for further European support initiatives

In general, the approach focussing on data sharing by authentic sources seems the most appropriate, cheapest and the most functional. The Polish legislation on the PSC has generally chosen this path, both downplaying the production of separate (derivative) documents and eliminating necessity to submit them in relations with the government. This trend is advisable on the European level also, thus shifting the perspective from the recognition of documents to the interoperability of generic networks.

As a separate matter, the degree to which the front-office relations restrict electronic authentication by requiring the most secure, but also the most expensive, type of electronic signature is confusing, considering that secure electronic signatures verified with qualified certificates have neither been accepted by the market in commercial relations, nor have they been appreciated by eGovernment customers so far. Thus it might be recommendable to promote flexibility in the authentication methods on the European level, to invite cheap and functional methods of authentication prevailing in commercial relations, like the credit-card authentication, among others.
27 Portugal

27.1 General framework for electronic documents in eGovernment applications

27.1.1 Electronic documents in eGovernment applications

Portugal does not have a generic framework related to electronic documents in eGovernment applications in general. While a relatively large number of eGovernment applications are available to the public, they are regulated and implemented by each public department.

There is however a new trend leading to Portuguese applications relying on electronic documents. Nevertheless, this approach has not yet been consolidated and, in particular, no specific technological tools or systems have been defined to implement the communication between public authorities and the interested parties.

Although paper communications are still the major form of proceedings carried on by the administration, we must indicate that since 1999, by the Decree-Law 290-D/90, the Portuguese legal framework expressly states that public entities may issue electronic documents bearing a qualified electronic signature pursuant to the provisions of this statutory instrument for “operations that concern the creation, issuing, storage, reproduction, copying and transmission of electronic documents, which formalize administrative acts through computer systems, including the transmission thereof by telecommunications means. The data relating to the interested entity and the person who carried out each administrative act shall be indicated in clearly identifiable language and in a manner that will enable verification the functions or the position of each document’s signatory” (Art. 5). From this statement, it is clear that Portugal intended to provide a legal solution for the use of electronic signatures in the general act on electronic documents.

Generally speaking, electronic documents are not issued to end users or requested from them in the context of eGovernment applications, and this is unlikely to change in the near future.

565 Although the current practice is that we are facing a continuous use of email to mere communication by the public authorities – this means outside the scope of the administrative act, the most relevant acts.
27.1.2 Electronic documents for the purposes of the implementation of the Services Directive

The Simplex\textsuperscript{566} project (Legislative and Administration Simplification Program - simplification and dematerialisation procedure carried on by the Government) is the major guideline followed by the government in the simplification and dematerialisation proceedings, including for the purposes of the Services Directive.

This means that there is not a strict focus at this time on observing the Services Directive rules (and namely the article 8). Nevertheless, there is a concretisation of this European provision within the environment of Simplex. We must also refer that the enactment of the new Public Contracts Code is, in our opinion, a new spot contributing to the implementation of PSCs.

Please note that, due to nature of the administrative division of Portugal (Portugal is a country without administrative regions), there are no major constraints in the adoption of central PSCs: and in fact, all the main services are provided on a country wide basis and the trend is to use electronic platforms to incrementally diminish the relevance of the geographical competences of bodies.

There are (or it is planned to be implemented by the end of the year) several web solutions that implement PSCs in a limited form. We can refer specifically to the following initiatives:


It should also be noted that the mentioned Code allows public entities to acquire assets regulated by Decree-Law nº 197/99 through electronic means.

The major principles of the act on the area of PSCs and electronic communication between the administration and the interested parties are\textsuperscript{567}:

(a) Public procurements are published on an Internet portal through an announcement in accordance

\textsuperscript{566} On March 26, 2006, the Portuguese Government launched a global program for administrative modernisation called "SIMPLEX - Programa de Simplificação Administrativa Legislativa" (Simplex - Legislative and Administrative Simplification Programme) which included the introduction of 333 new measures to simplify the administrative obligations of companies.

\textsuperscript{567} Please note that since the Decree-Law no. 104/2002, of 12 April (this act approved the electronic purchasing of goods by public organisms), it has also been implemented some preliminary actions in order to test e-Procurement solutions. The new Code revoked this act.
with the official model and in processes that imply an announcement in the Official Journal of the European Union, these should be electronically sent to the Official Publications Service of the European Communities.

(b) In negotiation processes, the jury can inform the candidates through any electronic means of data transmission and all of the formalities of the negotiation process may be based on electronic means of communication.

(c) During the process of competitive dialogue, the jury can notify qualified candidates through any electronic means of transmission of data. Furthermore, Electronic auctions are included in a specific section.

(d) The electronic auctions obey by the following regime: (i) All of the commissioning entities may make use of the electronic auctions, for commissioning preparation purposes (in the event that the proposal attributes only when depicted in a quantitative value and evaluation through an automatic mechanism). (ii) All the candidates whose proposals were admitted will be invited simultaneously by the commissioning entity, through electronic means, to participate in the auction. (iii) The auction may be processed in consecutive stages, each one corresponding to the bid value of each of the attributes, if there are several, of the proposals on electronic auction. Furthermore, the commissioning entity cannot, at any given moment, reveal the identity of the candidates in the course of the auction.

(e) Dynamic Acquisition Systems are also set forth, in that Public entities may, through a electronic system, namely an electronic management platform, conclude contracts for purchasing goods or services destined for current use with standardised technical specifications.

Although there has been some delay in the implementation, it is expected that the system will be subject to the following: (i) Any interested party may access the system through the presentation of an initial version of a proposal. (ii) The dynamic acquisition system will be made operational in the following phases: (1) system implementation; (2) simplified announcements; (3) actual awarding.

(f) The commissioning entity must make available the terms of the procedure on the Internet portal or on an internet page of their responsibility.

(g) The documents to be presented by the interested parties in access system. These should be submitted through electronic means, except in cases where this is not possible due to the nature of the documents or because of occasional failure of the computer equipment, hence not of the responsibility of the interested parties.

Please note that the electronic communications, exchange and database archive principles and rules if the Public Contracts Code have been regulated by the Decree-law 143-A/2008, of 25 July and several development Administrative Orders (such as the Administrative Order n.0 701-G/2008) in this field.

This Decree-law 143-A/2008 sets out that the e-platforms of the public entities must comply with several requirements, such as interoperability, compatibility, confidentiality and security with the
“Base” platform (please see below). The Administrative Order n.o 701-G/2008, of 29 of July, defined some of the requirements of the platforms of the public entities (through which the interested parties will apply the respective proposals), being the most relevant for this study the need of the interoperability of the public entities e-platforms with the site Base, of the Imprensa Nacional da Casa da Moeda (INCM) and the ICI.

After 1 January 2009 all public procurements must be carried out by electronic means, but it seems likely that the majority of public entities are not prepared to such a step, as the transitorily timeline of 4 months is considered to have been very tight.

On the other hand, some of the objectives of the Code will also be achieved by the Public Purchasing National System (SNCP- Sistema Nacional de Compras Públicas), system regulating the creation and approval of the Public Purchasing National Agency’s statutes (ANCP).

The Public Purchasing National System\(^{568}\) is governed by the Decree-Law no. 37/2007, of 19 February, which also defined the National Public Purchases Agency, E.P.E. (ANCP- Agência Nacional de Compras Públicas), which will integrate all of the current purchasing entities by law, and will allow other voluntary purchasing organisms to accede to the system.

In addition there is the National eProcurement Programme (PNCE), which outlines the following main objectives:

- To promote the efficiency of the process of public acquisition: i) generating structural profit and savings; ii) facilitating and expanding company access to the public purchasing market; iii) increasing the transparency and quality of the service provided.

- To grant economical agents with modernisation dynamics: i) promoting their competitiveness and productivity; ii) encouraging the adoption of new e-commerce practices on a national level.

This National Program launch the Catalogue Management Central System\(^{569}\). The Catalogue Management System is a central repository of products and services from State suppliers allowing the Public Sector buyers to conclude the acquisition processes, optimising their business relationship and model, containing general information on products and services for the Public Sector as well as useful specific information on the procedures of public acquisition. The supplier will have to submit the information related to their products and services and with the necessary regularity carry out the administration and maintenance of that data.

---

\(^{568}\) The Public Purchasing National System is built on the following platform: (i) Integration of all of the current purchasing entities by law, as well as other voluntary purchasing organisms on a contractual basis; (ii) Segregation of contracting and purchasing functions and the adoption of centralised payment procedures, on both a global and sectorial level, on a frame agreement or other public contracts and in the subsequent purchase and payment by the purchasing entities; (iii) Hybrid model for SNCP management.

\(^{569}\) It is a system built on the platform of the Public eProcurement Technological Model, defined in a partnership forged with the HPG Group Company and having the Catalogue Management System as the one who primarily interacts and interoperates with the National Suppliers Registry and other internal and external systems, such as e-commerce service providing companies (B2B).
This is the general environment on the public procurement.

Now, the portal designated by the Code is a public announcement website bringing all official public announcements and adverts together on a single website with universal free access for individuals and enterprises. This web platform ensures that information is publicised in a systematised way, allowing every announcement or advert to be consulted by issuing body, date, or subject matter. The portal is accessible at http://www.base.gov.pt/Paginas/Default.aspx (“Base”).

Base gives access to the IT systems now being introduced to receive, structure and process data on the formulation and implementation of public contracts for the purchase or rental of goods and services, public works contracts and the contracting out of public services. Information from the online version of the official gazette will gradually be fed into the databases linked to the portal, together with material from other eGovernment platforms and, from now on, the inputs sent directly to Base. In this way, a “state-of-the-art” knowledge base on Portugal’s public contracts will be built up.

So the main function of Base is to publish the information required by the Code, namely contract calls, contract signings, contract modifications representing more than 15 % of the price, and any decisions to withdraw a tenderer’s right to take part in public pre-contractual processes, as a sanction.

In 2008, regarding the scope of the art. 8 of the Services Directive, the Simplex program lead also (in certain cases, projects are not completed) to the following projects:

**New Website for Electronic Edition of the Diário da República**570

The new site reformulates the website of the Electronic *Diário da República* (the Official Gazette). This platform has new functions making it easier for individuals and enterprises to access legislation and published official acts.

**Payment of VAT on imports**571

The previous site, that was a PSC for the VAT payments, has now new solutions, simplifying the procedure for paying VAT on imports by dematerialising the receipt. The site now also allows: (i) Economic operators (taxpayers) to ask for the declaration proving that they have paid VAT for a given period to be issued on the Internet by the Directorate-General of Customs and Special Taxes on Consumption (DGAIEC). (ii) Operators to exercise their right to deduct tax paid using this dematerialised declaration, without having to physically go to the customs services.

---

570 [www.dre.pt](http://www.dre.pt)
Driving licence\textsuperscript{572}

The platform makes it possible to electronically apply for the revalidation of a driving licence or the issue of a replacement one, inform the authorities of a change of address, and pay fees. The idea is to do away with the need for people to physically go to the Institute of Mobility and Terrestrial Transport (IMTT), reduce the average time taken by the various procedures, and reduce the number of complaints.

Contacts with the Social Security System\textsuperscript{573}

It has been created a national Social Security Contact Centre based around a telephone service, but also including the e-mail, fax and Internet channels (expected to begin with a pilot project in December 2008).

Casa Pronta (Fast-Track Home Buying Scheme)

The main aims of Casa Pronta (Fast-Track Home Buying Scheme) are:
\begin{enumerate}
\item To eliminate formalities and bureaucracy during the transfer and assignment of real estate;
\item To complete all the necessary procedures in a one stop shop (celebrating a contract, paying taxes, registering property, etc).
\end{enumerate}

Casa Pronta was launched in June 2007 in 5 municipalities. After an experimental phase, which should be concluded by the end of 2007, the scheme will be rolled out nationwide.

The PSC portal is www.casapronta.mj.pt

Civil Governments (Governos cívis)

For December 2008, it is planned a website refreshment in order to assure users the fulfilment and electronic application of some forms, namely registration of fires, associations, authorisations of advertising passtimes\textsuperscript{574}.

Furthermore, there are plans to implement the notice and the communication of decisions by electronic means. No further information has been provided about targets or timelines.

\textsuperscript{572} http://www.dgv.pt/formularios/formularios.asp
\textsuperscript{573} http://www2.seg-social.pt/
\textsuperscript{574} http://formularios-governoscivis.mai-gov.info/
27.2 Specific document types

27.2.1 Extracts from commercial registers

Decree-Law no. 125/2006, of June 29, establishes a way to incorporate companies through the Internet. This act has been regulated by the Council Order no. 657-C/2006, of June 26.

As noted above, electronic documents are not normally used by Portuguese administrations, and the re-use of authentic sources is much favoured. The commercial registers are a key example of this.

However, it has been fully implemented an online service regarding the permanent certificate of the company ("Permanent Certificate"). The Permanent Certificate discloses the legal information of any company in order to ensure the safety of its transactions, thus it’s the online service which enables the access to the day-to-day updated status of all the registries of companies registered in Register Offices (companies, cooperatives, State-owned companies and other entities with commercial registry).

This service allows any entity, whose record is in the database of SIRCOM (Information System of Commercial Registry), to have a Permanent Certificate always available through the Internet, assuring that while this certificate is online, no entity, public or private, can demand a paper certificate.

The Permanent Certificate contains all the company’s registries, including the requests by transcription or deposit pending on drafting or confirmation. Regarding the latter, you are given information on the presentation and/or deposit number, plus the type of registry requested.

The permanent certificate can be issued through the Internet at\(^{575}\):

- [https://www.portaldaempresa.pt](https://www.portaldaempresa.pt);
- [http://www.empresaonline.pt](http://www.empresaonline.pt);
- [http://www.mj.gov.pt/publicacoes](http://www.mj.gov.pt/publicacoes);

This service can be applied by anyone and does not require any type of authentication.

Technically, the Permanent Certificate which has expired can not be renewed. Its access code is automatically deactivated except for those whose request is pending (without confirmed payment). In these cases, the Permanent Certificate can still be consulted up to a maximum of five days. Nevertheless, when renewing the Permanent Certificate, the access code remains the same.

\(^{575}\) The certificate can also be applied in any Commercial Register Office (in this case, by the presence of the requesting party).
27.2.2 Criminal records

Excerpts from the penal register exist in Portugal, but with one exception (referred below) only in a paper format. The extract is provided by the local commune of domicile for natural persons.

The criminal registry collects and organises information about all criminal sentences issued by Portuguese courts and about sentences issued by foreign courts applicable to Portuguese citizens and foreigners residing in Portugal.

A criminal record certificate may be requested in person by the party in question at various locations (e.g. Lisbon criminal identification services, Citizen Shops (Lojas do Cidadão), courts, etc.), but always through a physical petition submitted in person who shall also present the respective identification card. The petition may also be requested by a third party with powers for the purpose (and with the associated documentation, including the petitioner’s identification card or the respective certified copy).

However, it may be legally required to submit a criminal record certificate for certain administrative procedures (e.g. employment or for obtaining a licence, authorisation or record of a public nature). When such is required, the public entities competent to process that administrative procedure are authorised by the Directorate-General of the Justice Department to receive criminal record certificates electronically if the request to issue the certificate is submitted to those public entities.

Consequently, through Decree-Law 20/2007, of January 23, and according to the Simplex Program, a citizen’s current obligation to obtain a criminal record certificate was transferred to the public entity responsible for processing administrative procedures which legally require the said certificate. That legal statute was implemented through Ordinance no. 170/2007.

A request for an electronic criminal record certificate is forwarded electronically to the criminal identification department by filling out the appropriate electronic form provided by the said department for the purpose.

When the properly filled out electronic form specified in article 8 has been received by the criminal identification department, it will:

a) Issue the requested criminal record certificate and send it by mail to the public entity that submitted the request;

b) Through the most appropriate means, will request any essential additional information for making a decision regarding the respective certificate.

http://www.mj.gov.pt/sections/pessoas-e-bens/registro-criminal/index/
http://www.dgaj.mj.pt/DGAJ/sections/home
Note that a password identifying the work station and person accessing the system is necessary to electronically forward the criminal record certificate request and to electronically receive the negative criminal record certificate.

In conclusion, despite the trustworthy framework already stipulated, this is a recent procedure which is still in the implementation process.

### 27.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations, orders or stakeholder bodies. While it is difficult to obtain a complete overview, it does not appear that the extracts issued by such private organisations are commonly issued in a paper form. The legal possibility to do so exists, due to the implementation of the Signatures Directive, but in practice only paper documents are commonly issued. In instances where electronic documents are made available to the members of a specific profession, this is typically only done in the form of paper copies, notably PDF scans of the original documents.

Currently, no plans exist to make the use of electronic documents mandatory or to encourage them further.

Please note however that many professionals (such as lawyers, solicitors and notaries) have the power to certify documents and the Layers Bar Association and Notaries Bar have already implemented PKI platforms issuing digital signatures to their members.

The technical solutions spreading the use of electronic signatures and the legal effect of electronic documents (electronic documents have the same effect as hard-copy documents), in our opinion allow the dematerialisation of this type of documents and thus, the implementation of electronic extracts from professional registers.

### 27.2.4 Certificates of insurance

---

578 In order to provide lawyers with an appropriate certificate, the Portuguese BAR Association (http://www.oa.pt/) entered into two Protocols in 2003 with Multicert - Serviços de Certificação Electrónica, S.A. (http://www.multicert.pt/): the first for the provision of digital signatures and the second for the provision of MDDE, a solution that combines the issuance of digital signatures and time stamping.


580 In fact, the use of electronic signatures has been recognised under Portuguese law since 1999 (Decree-Law no. 290-D/99, of 2 August - legal regime for electronic documents and electronic signatures) and according to art. 7 of Decree-Law no. 290-D/99, electronic signatures constitute valid proof of declaration with the same value as handwritten signatures.
Certificates of insurance are not issued in an electronic form. As previously sustained, the full application of Art. 3 and 7 of Decree-law no. 290-D/99 should lead us to the conclusion that this requirement is met even if the certificate of the insurance is issued by electronic means and signed by a digital signature.

Furthermore, the law of insurance (Decree-Law n.o 72/2008) makes no mention to the fact that the insurance contract must be in paper form (i.e. this is not a formal contract under Portuguese law). As the validity of this contract is not subject to any form, these contracts can be executed orally or in writing. Since it does not have to be in writing, obviously there is no legal requirement establishing that it must be in paper form. So, in order for an insurance contract to be legally binding, all that is necessary is that the general regulations of Decree-Law no. 290-D/99 (art. 3 and art. 7) are complied with.

The only requirement is that the insurance company must provide the client with a written document (the certificate of insurance). Hence, there are no restrictions on issuing an insurance contract or the certificate of insurance by electronic means. As such, there is no legal barrier for the use of electronic contracts in the provision of the certificate of insurance.

Currently, no plans exist to make the use of electronic certificates of insurance mandatory or to encourage them further. For the purposes of Portuguese PSCs, the emphasis is mostly on ensuring that original documents are no longer requested unless this is absolutely necessary, in compliance with the administrative simplification obligations of the Directive.

### 27.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications: generally, these are private sector issued documents for which only paper originals are available. While electronic copies might occasionally be presented in the form of unsigned scans, this is merely a matter of convenience. No specific rules or framework exist for electronic proofs of qualification beyond the general eSignatures Act, and no plans have been proposed to encourage or mandate their uptake.

### 27.2.6 Statements from the service provider

Statements made by the service provider himself will likely be integrated into the websites of the PSC as web forms to be completed and signed. It is not yet clear which requirements will be imposed on such statements, beyond the comments made above.
27.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

27.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

Within the scope of Simplex project, many of the services are being analysed in order to be simplified and to provide users with a PSC.

Due to nature of the administrative management of Portugal, all the main services are provided on a country basis and the trend is to use electronic platforms to increment diminish the relevance of the geographical competences of bodies.

27.3.2 Commercial registry

Decree-Law no. 125/2006, of June 29, establishes a means of incorporating companies through the Internet. This act has been regulated by the Council Order no. 657-C/2006, of June 26.

The adopted regime for incorporating commercial companies or private companies having a commercial form through the Internet may be used by any interested party, be they natural persons or legal entities, represented by the relevant persons in charge, with sufficient powers in the company.

In addition, also lawyers, solicitors and notaries may promote their constitution, certifying the identity, capacity, representation powers and the will of interested parties, using a means of electronic validation of their identity.

The web sites for this purpose are www.empresaonline.pt, to be maintained by the Direcção-Geral dos Registos e do Notariado (Directorate-General for Register and Notaries) and http://www.portaldaempresa.pt.

The incorporation of companies by this e-Government platform is made by lawyers, solicitors and notaries, being the electronic authentication made through the use of a digital certificate that evidences the professional quality of the user — these certificates must only be used for professional purposes, as evidenced by electronic lists of certificates made available, respectively, by the Ordem dos Advogados (Lawyers Bar Association) the Câmara dos Solicitadores (Solicitors Association) and the Ordem dos Notários (Notaries Order).

581 On March 26, 2006, the Portuguese Government launched a global program for administrative modernisation called “SIMPLEX - Programa de Simplificação Administrativa Legislativa” (Simplex - Legislative and Administrative Simplification Programme) which included the introduction of 333 new measures to simplify the administrative obligations of companies.
During the online establishment of companies, each applicant must use its qualified electronic signature on the statutes or instrument of constitution of the company.

The platform enables the following:

- The authentication of users through digital certificates;
- The identification of the data of interested parties;
- The choice of business name created and reserved in favour of the State beforehand;
- Examination as to the admissibility and acquisition of a business name, pursuant to paragraph 3 of article 45 of the regime of Registo Nacional de Pessoas Colectivas (RNPC) - National Registry of Legal Entities;
- Indication of the business name included in the business name admissibility certificate issued by the RNPC;
- Choice of and filling in of statutes or instrument of constitution of a model approved by the Director-General for Register and Notaries, or for submitting statutes or instrument of constitution prepared by interested parties;
- Electronic completion of elements necessary for the presentation of the declaration concerning the taking up of activity for tax purposes;
- Submission of documents necessary for the assessment of the application and to correct any shortcomings;
- Electronic signature of documents delivered;
- Electronic payment of services;
- Collection of information enabling the communication between competent services and interested parties and their representatives;
- Application for commercial registration of company constitution;
- Certification of date and hour when the registration was executed;
- Access to the website where the legal publications are made available.
- Interested parties shall also submit through the Internet website the following documents, among others, :
  - Documents supporting their capacity and powers of representation for the act;
  - Special authorization required for the setting up of the company.

The application submitted shall be deemed to be validly carried out provided that an electronic supporting document is issued, through the Internet website, that indicates the date and hour of registration.

The service shall manage such data and any documents delivered by interested parties.

The competent service shall take the following steps:

- To register the statutes or instrument of constitution, and to immediately communicate such registration to interested parties by electronic means;
- To record this fact in the central file of legal entities and economic activity code, or when appropriate, to communicate the registration for this purpose;

The competent service shall also to provide the following:

- To issue and to send to interested parties the legal entity identification card and the certificate of payment of charges due, as well as to communicate thereto the company's identification number at the social security;

- To provide, free of charge, evidence of the company's creation registration, pursuant to and through the means provided for the Commercial Registration Code;

- To promote computer-based legal publications, which shall take place automatically;

- To provide the competent services, by electronic means, with the necessary data for the control of tax obligations, with the necessary data for the purpose of informing Inspecção-Geral do Trabalho (General Labour Inspectorate) the companies activity, as well as with the necessary data for the official entry of the company in the social security services, and, when appropriate, in the Commercial records;

- To promote all other measures established in regulations or protocols;

- To send the company's portfolio to the commercial registry office having territorial jurisdiction, pursuant to the Commercial Register Code.

The remaining documents submitted in the course of the procedure must bear the qualified electronic signature of the interested party sending the documents, unless a lawyer, solicitor or notary is responsible for such submission.

The documents submitted shall be digitally signed by the receiving computer system and the receipt sent to the applicants via e-mail. Finally, the registration of the company's statutes or instrument of constitution must be notified to interested parties via email, and if appropriate by short message service (sms).

27.3.3 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Legal measures leading to a new step on the communication between the Point of Single Contact and the service provider have not yet been taken. As mentioned, for instance, within the scope the commercial registration, the administration notifies the parties via email, and if appropriate by short message service (sms).

At this moment, it has neither yet been decided, nor we may see a trend to the management of such a communication.
27.4 Assessment – Plans, progress and proposals for further harmonisation

27.4.1 Current plans and progress in the implementation of the Services Directive

The national program “SIMPLEX” is the initiative highlighting almost all the public activities around the dematerialisation purposes and the implementation of more advanced electronic platforms. We are of the opinion that the mentioned program will continue as the mentioned program is a political flag of the Portuguese Government.

Although simplification cannot simply be brought about by decree (and it should be looked at as a general strategy based on ongoing actions designed to constantly assess and correct administrative rules, standards and practices), the fact is that the relevance of such a program along with the enactment of the new Public Contracts Code (entering into force in 2008) will develop the use of electronic platforms and can be a boosting scheme for a new mindset.

Nevertheless, the focus on the Simplex project leads to the idea that there is a national dematerialisation project that encompasses the scope of the Services Directive, but in no case, the mentioned European Directive is seen as a driver for the development of electronic environment or the changes of the law.

This approach also affected our work as we did not have a centralised entity with the ownership of implementing the Directive.

27.4.2 Suggestions for further European support initiatives

The Portuguese legal environment already contains a material set of provisions allowing implementing dematerialised structures and PSCs. An important work is still to be carried on, though.

Our suggestions to European initiatives derive from the major issues that we believe are still constraints to a full development in this area in Portugal.

---

582 The major purposes of this plan are: “The idea was to lead public departments and services to constantly review their interactions with individuals and enterprises, to assess the costs of each of those interactions and the burdens they imposed, and to ask whether they were useful and relevant… This effort must help to increase people’s trust in public services and public servants by facilitating their daily lives, the exercise of their rights and the fulfilment of their obligations, and reinforcing the protection of their fundamental rights… It must enable enterprises to quickly obtain permits and authorisations and fulfil other formalities they need in order to get on with their business, or dispense them from such procedures when they are proven to be useless.”
- e-Legal culture: Many citizens still do not rely in electronic documents. We consider that it should be carried on a strong effort in adapting the legal framework in order to drop away the references and the use of paper environment and giving citizens a sign that electronic documents are a solution that should not be disregarded.

- Contents: Many portals (in the area of the public environment) are not fully updated. This means that users cannot always rely on the provided information. Obviously the production of contents and the update of those contents imply the use of resources, but attractive and updated contents are the core issue for the success of a portal and the best solution to users being attached to such a service.

We consider that: (i) the gap of information on portals should be analysed; and (ii) the allocation of sufficient resources on the production and update of contents should be promoted.

- Language: the multitude of languages leads to barriers on how to extend the information to users of other countries. We consider that some essential portals should provide translations of contents into the English language, at least in relation to the most important contents.
28 Romania

28.1 General framework for electronic documents in eGovernment applications

28.1.1 Electronic documents in eGovernment applications

At the national level, Law no. 161 of 2003 regarding Certain Measures for the Ensuring of the Transparency in the Exercising of Public Positions, Public Offices and the Business Environment, Prevention and Punishment of Corruption, as updated in May 2007, ("Law no. 161") provides a general framework related to the electronic procedure applied by the authorities in relation to natural persons or legal entities.

The e-Government applications available to the public are regulated and implemented as provided by Law no. 161. Title II of Law no. 161 regulates the National Electronic System (in Romanian Sistemul Electronic National, SEN), ("NES") as a central point of access to information and electronic services of the public administration, offering users a set of electronic services, access to administrative forms and procedures, and access to contact points for local and national authorities.

NES contains two components: the e-Government System (in Romanian e-guvernare) and the e-Administration System (in Romanian e-administratie); however only the e-Government is available online\(^{583}\).

The e-Government System consists of a website which ensures the interoperability between the e-government applications at the national level by using a software platform\(^{584}\) to provide secured data transfer between public authorities, as well as between public authorities and the end users. The website is based on pilot projects, first developed in 2002, by the Ministry of Communications and Information Technology.

The website has two sections. On one hand, it provides the download of standard forms used by different authorities, which can be filled in, printed and sent via traditional mail, or filed directly (on paper) with the relevant authority. On the other hand, the same standard forms may be filled in electronically and sent online.

---


\(^{584}\) The NES - SDK (in Romanian SEN-SDK) represents a collection of documents, code examples, test electronic services and software libraries necessary to integrate NES's standardized authentication and secured communication services with third party software applications belonging to natural persons or legal entities or to the public authorities.
The most important online service provided by NES is the Unique Form System. Currently the Unique Form System integrates nine online applications. The number is expected to progressively extend according to the Decisions issued by the Government. The Unique Form System represents the first step towards the implementation of the Services Directive, as it is the first online service which facilitates the communication by electronic means between a service provider, natural person or legal entity, and a public authority.

There are legal provisions regarding certain e-government services which impose a standardized format for electronic documents, based on .pdf formats of documents (e.g. fiscal declaration with the National Agency for Fiscal Administration), company registration with the National Trade Registry. However, for most e-government services (local and central level) there is no national standardisation for electronic documents yet.

With regard to specific requirements for electronic signatures, in addition to the compliance with the provisions of the e-signature national legislation, Qualified Electronic Certificates (“QEC”) will be required in order to sign electronically, for the implementation of the Services Directive.

While the technical requirements for the use of the NES are not directly enforced by legislation, Law no. 161 provides that the Ministry of Communications and Information Technology and the Ministry of Internal and Administration Reform shall lay down such procedures and technical norms.

Law no. 161 also mentions that all documents sent and received by using the electronic procedure must have an electronic form and must be signed electronically as established by the operator of the e-Government System, i.e. the Agency for Information Society Services (in Romanian Agentia pentru Serviciile Societatii Informationale, ASSI), (“AISS”).

So far, the AISS has not issued any regulations regarding the technical requirements, however on the www.e-guvernare.ro site guidelines were posted for registering and using the website for each service provided.

Public Authorities using NES may post electronic standard forms. According to the information available on the website, the standard forms have to be in .pdf editable format (not mere images) compatible with Adobe Acrobat Reader 4.0, or .doc compatible with Microsoft Word ‘97. The Properties section has to be filled in with information regarding: Name, Author, Subject, Key Words.

The guidelines regarding the Unique Form System specify the technical requirements for the use of the service. Windows98/NT/2000/XP/2003, Microsoft Internet Explorer 6.0 Browser with Service Pack 1, and Microsoft .NET Framework v 1.1 are required.

---

585 According to the provisions of the Government Decision no. 1085 of 2003, all Public Authorities have the obligation to register and use the NES. The said Decision also provides a list with all the authorities which have to use NES, a list with the public services provided by NES, and a list with all the standard forms available through NES.
Currently, the national interoperability framework implemented in NES does not standardise the formats of the documents. As mentioned by the representatives of the Agency for Information Society Services, Romania is actively participating in the workgroups coordinated by the European Commission in view of the elaboration of common specifications for electronic signatures, electronic documents, and other issues in the process of the implementation of the Services Directive.

28.1.2 Electronic documents for the purposes of the implementation of the Services Directive

For the implementation of the Services Directive, a specific legislation providing the legal requirements which are to be imposed is under development. In view of the implementation of Art. 8 of the Services Directive, the Department for European Affairs of the Romanian Government drafted and posted on its website for public debate the draft of the Government Ordinance ("Ordinance") to be issued by the Romanian Government regarding the implementation of the said directive. The national primary legislation, i.e. the Ordinance, is in a final stage, being submitted to public discussions. It is expected that the said ordinance will be approved and issued in January 2009.

According to the draft of the Ordinance, an Electronic Point of Single Contact ("Electronic PSC") will be set up. However, it is also specified that such set up of the Electronic PSC will not restrict in any way the setting up or operation of physical sole desk offices.

The Electronic PSC shall have the status of public utility informatics system and will be an integral part of the E-Government System of NES, being governed by the provisions of the Title II of Law no. 161.

The limits of the competence of the Electronic PSC operator, the detailing of the operational mechanisms and of all activities carried out through the Electronic PSC, as well as the financing means necessary for the operation of this system shall be established by Government Decision, without conflicting with the provisions of the Ordinance, and/or the relevant European Community legislation. Such secondary legislation is under development.

The draft of the Ordinance provides that the electronic PSC shall become operational by November 28, 2009.

The functioning of the Electronic PSC shall not prejudice the competences of the Romanian public authorities, of the professional bodies, or of other bodies having regulatory, authorization, or control powers in the field of services.

According to the draft of the Ordinance, through the Electronic PSC, the providers will easily carry out, remotely and by electronic means, the following procedures and formalities:

(i) all the procedures and formalities necessary for the access to the services activities thereof, mainly all the statements, notices or applications necessary for the issuance of the
authorization from the competent authorities, including the application for the registration with a register, with a database, or with an order or professional association;

(ii) any applications for authorization necessary for the carrying out of the activities.

The obligation to register and use the Electronic PSC is restated in the draft of the said Ordinance. The competent authorities must perform the registration within 30 days as of the date the Electronic PSC becomes operational.

According to the draft of the Ordinance, the following information will be accessible to the service providers through the Electronic PSC:

a) the applicable requirements of the providers registered in Romania, mainly regarding the procedures and formalities which must be complied with in order to have access to the services activities and to exercise them;

b) the contact information of the regulatory authorities, necessary in order to contact them directly;

c) the means and conditions for accessing the public registers and databases regarding information about the providers and the services;

d) the legal actions generally available in case of a dispute between the competent authorities and the provider or beneficiary or between a provider and a beneficiary or between providers;

e) the contact information of the associations and organizations, other than the competent authorities from which the providers and the beneficiaries can obtain practical assistance.

By accessing the Electronic PSC, the services providers, natural persons or legal entities, may receive, upon request, assistance from the competent authorities, consisting of information with regard to the interpretation and application of the procedures and formalities which must be complied with in order to obtain the authorization and to carry out the activities.

The competent authorities have the obligation to answer to any request for information by means of Electronic PSC, within five working days at most. The draft provides that, in the cases when the request is erroneous or lacks a legal basis, the authorities have to inform the applicant accordingly, within the shortest period possible, but not exceeding five calendar days.

Also it is mentioned that the obligation of the competent authorities to assist service providers and beneficiaries does not mean that the said authorities are compelled to provide legal assistance in individual cases, but concerns only general information with regard to the manner in which the requirements are commonly interpreted or applied.
The AISS is responsible for the technical operation of the Electronic PSC. The authorities will be liable for the content of the information and documents collected, sent and processed through the Electronic PSC.

Specific technical requirements were elaborated and included in a technical project drafted by AISS which was submitted for Structural Funds. The project is currently confidential. Detailed technical specifications will become available to the public at the beginning of 2009, after the approval of the funding.

With regard to the acceptance of electronic documents, including those from service providers of other Member States, three possible situations can be anticipated:

(i) the service provider sends via the Electronic PSC an electronic document signed with an electronic signature.

(ii) the service provider sends a scanned copy of the signed original document which will be signed electronically by the service provider and also by the authority/administration which issued the said document. The electronic signature of the administration will be validated by checking the Trust List where the authority is registered.

(iii) The document provided is signed by an authority which is not on the trust list.

The above-mentioned situations are still under debate in the workgroups coordinated by the Commission, any decision in respect thereof will be applied also to the delivery of electronic documents in Romania.

A certain level of interoperability between the competent authorities of the Member States will be achieved by the Internal Market Information System (IMI). According to the draft of the Ordinance, the competent authorities have to register with IMI. The local authorities may file applications through IMI with the authorities of the Member States regarding the investigation of service providers or to obtain additional information about the service provider.

The AISS, which is the Romanian public institution responsible with the implementation of the Electronic PSC, undertook important steps in view of the setting up of the Electronic PSC, such as participating in the elaboration of primary and secondary legislation for the implementation of the Services Directive, elaborating the concept of the Electronic PSC, the detailed functionalities list of the Electronic PSC. As mentioned above, the AISS drafted the technical project regarding the Electronic PSC and filed it in order to obtain Structural Funds for its implementation.
28.2 Specific document types

28.2.1 Extracts from commercial registers

In relation with the Romanian authorities, electronic documents were scarcely used in the past, in favour of original documents.

In order to increase the use of the electronic documents, in January 2008 the Trade Registry set up the Intelligent Electronic Application System, in Romanian: Sistemul de Formulare Electronice Inteligente\textsuperscript{586}. By using this system, a company can be registered by filling in an on-line application which shall incorporate an extended electronic signature. All the documents supporting the application for registration will be filed in scanned copies.

All information related to economically active independent entities in Romania is stored in the National Trade Registry database. The said information is available on line\textsuperscript{587}, on the National Trade Registry online database, i.e. RECOM. The said database provides without charge the information regarding the full name of the company, registration number, sole registration code, and the registered address of the company. Detailed information regarding a company is for a fee.

Although the details of a company are available through web interface, printed extracts of such database cannot be used before the authorities, as they are not signed or stamped accordingly. Therefore, the official extracts and the certificates of good standing are currently issued by the Trade Registry only in hard copies, and only the original can be used before the authorities.

Basic information about the entities stored in the Trade Registry database includes:

- Full name and legal form;
- Registration number with the Trade Registry;
- Sole registration code;
- Registered address and date of registration;
- Registered activities according to the National Classification of Activities, \textit{CAEN};
- Details regarding the Shareholders;
- Details regarding the Managers;
- Shared capital;
- Basic financial information, the date of deposit of the balance sheets;
- List of registered work sites in Romania.

\textsuperscript{586} See \url{http://e-forms.onrc.ro/Register.do?l_activ=register}, (in Romanian)

\textsuperscript{587} See \url{http://recom.onrc.ro/indexe.htm}, (in English)
Pursuant to a recent Order no. 2594 of October 2008 (“Order no. 2594”) issued by the Justice Ministry, the issuance of certificates of good standing or of official extracts by the Trade Registries will also be possible electronically, via e-mail. Such certificate or extract will incorporate or will have attached an extended electronic signature, according to the Electronic Signature Law.

An application may be filed personally, by registered mail, or by e-mail in order to obtain an electronic certificate of good standing or an official extract of the Trade Registry.

According to Order no. 2594, the General Manager of the National Trade Registry will issue explanatory notes regarding the application or the provisions of the Order. Such explanatory notes will most likely set the technical standards with regard to the issuance of electronic certificates of good standing or official extracts.

Currently, there are several approved technical standards for the electronic signatures, notably PKCS#7 and CAdES. The validity of electronic signatures is determined by using both CRL and OCSP. According to the representatives of AISS, the rules regarding the time stamping are in the final stage of approval.

### 28.2.2 Criminal records

Certificates of Criminal Record are issued in Romania only in a paper format. Such certificate is provided by the local Police Inspectorate where the natural person has his/her domicile.

Although the Criminal Code of Romania was amended in order to provide that legal entities may also be the subject of criminal investigation, the Criminal Records Law has not been further amended. Therefore, no certificates of criminal record are issued with regard to legal entities. In practice, legal entities are required to submit an affidavit authenticated by a public notary regarding the compliance with the relevant Romanian legal provisions.

The Ministry of Internal and Administration Reform proposed the amendment of the Criminal Records Law and drafted an Ordinance amending the Criminal Records Law in this respect. The Ordinance was not approved so far.

In some counties, the possibility exists to request the issuance of a Criminal Record Certificate electronically by filling in an on-line form on the local Police Inspectorate websites. However, the Certificate of Criminal Record is still issued in a paper format and delivered to the applicant or his representative who comes at the local Police Inspectorate Office. The on-line filing of the application to obtain such certificate is not commonly used mainly because currently the local Police Inspectorate issues the Criminal Record Certificate on the spot.

---

588 Order no. 2594 of October 10, 2008 issued by the Justice Ministry regarding the approval of the Application Norms re the Keeping of the Trade Registry Records, the Entry Execution, and the Issuance of Information. Such order entered into force starting as of November 16, 2008.
In view of the implementation of the Services Directive, the issuance of electronic Certificate of Criminal Records will be made available via the Electronic PSC.

28.2.3 Extracts from professional registers

Professional registers are typically managed by professional associations. It appears that the extracts issued by such private associations are commonly issued in a paper form, although the legal framework for their issuance in electronic format exists according to the Electronic Signature Law and to the Signatures Directive.

However, such professional registers are typically available online on the website of each professional association, and can be accessed free of any charge.

The use and issuance of electronic documents will be generally encouraged.

In addition to the general requirements for an electronic document, as the Romanian legislation provides that all the procedures and documents are to be filed/issued in Romanian language, simple or certified translations of the documents may be required.

28.2.4 Certificates of insurance

Although Art. 11 of the Insurance Law provides that the documents confirming the execution of an insurance agreement can be signed and certified electronically in accordance with the provisions of the Electronic Signature Law, usually, certificates of insurance are not issued in electronic form.

Recently a private insurance company launched an online service for concluding insurance agreements for travelling. The request may be filed online by filling in the application form and the payment can also be made online by using the e-payment service. The electronic certificates of insurance are delivered via e-mail.

Although the use and issuance of electronic documents will be encouraged, however, there are no plans for making the use of electronic certificates of insurance mandatory. In order to be accepted by the local authorities, the electronic documents have to comply with the requirements of the Electronic Signature Law, as mentioned above and also simple or certified translations of the documents may be required.

589 Art. 11 of the Law no. 136 of 1995 regarding Insurance has been amended in 2004 with regard to the issuance of electronic certificates of insurance
590 Law no. 455 of 2001 regarding the Electronic Signature
28.2.5 Proofs of qualifications

The same comments made above in relation to excerpts from the professional registers also apply to proofs of qualifications: generally, these are private sector issued documents for which only paper originals are available.

There are no specific rules for the issuance proofs of qualification in electronic format. However, after the implementation of the Electronic PSC, such proofs of qualifications will also be issued in electronic format, therefore simple or certified translations of the proofs of qualifications may be required.

28.2.6 Statements from the service provider

By accessing the Electronic PSC, a service provider may obtain all the forms which have to be filled and all the information in order to file an application for approval. The administration itself is managing the content, eliminating third parties', i.e. system operators, errors and delays.

With regard to the other documents in an electronic format, i.e. existing authorizations, company documents, requested by the administration in order to process an approval request, no standardised format is taken into consideration, due to the differences between administrations from other Member States.

The service provider will deliver its electronic statements through the Electronic PSC, using its private profile.

There are no specific provisions or framework for electronic proofs of qualification beyond the Electronic Signature Law. However during the implementation of the Electronic PSC, additional requirements may become necessary.
28.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

28.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As mentioned above with regard to the use of the NES, the interaction between the competent public administrations and the natural persons or legal entities is carried out through the e-Government website. As the Electronic PSC will be part of the NES, the interaction between the PSC and the competent public administrations or private organisations will be carried out through the PSC portal. The said portal will also facilitate the interaction between the authorities themselves.

When NES was set up, the Romanian Government provided a list with all Public Authorities which had the obligation to register and use NES, according to the Government Decision no. 1085 of 2003. The draft of the Ordinance regarding the Electronic PSC does not include this list. However, in Art. 2 of the draft, the activities to which the said Ordinance will not apply are mentioned, e.g. transport services, medical services, financial services, notaries.

According to the information provided by the representatives of the Department for European Affairs, more than 80 administrations and organizations will have to register and use the Electronic PSC.

Steps have been undertaken since 2007 in order to identify and inform all the relevant administrations and organizations which have to be linked to the Electronic PSC. This process is still ongoing.

With regard to the existence of an uniform delivery solution at the national level, the representatives of the Agency for Information Society Services mentioned that there will be a single electronic solution at national level, i.e. the Electronic PSC, which will provide support for all types of actors, such as service providers, administration, organizations.

The technical and organizational internal process will be managed by each administration or organization.

In respect thereof, certain aspects related to the delivery mechanism may require the amendment of the current regulations.

With regard to the advances/web-service oriented standards and communication protocols, currently several technical standards and protocols are already used in e-government systems, e.g. SOAP, secured XML.
The Electronic PSC will rely on open technologies, with a strong focus on open standards.

The draft of the Ordinance regarding Electronic PSC does not provide information with regard to the requirements for the registration and use of the Electronic PSC. As also mentioned above, the details of the operational mechanisms and of all activities carried out through the Electronic PSC will be established by Government Decision. Currently, the process is in progress. Its implementation will start in 2009, the funds for such implementation being ensured by Structural Funds.

28.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

With regard to the mechanism for the delivery of documents from administrations or private organizations to the service provider, certain aspects, such as response time requirements and liability, might require regulation, as the current framework does not provide for any solutions in respect thereof.

However, a technical project providing specific technical requirements for the delivery process, i.e. for sending replies for the service provider has been elaborated by the AISS. Reference has been made in the above-mentioned technical project to technical requirements that include but are not limited to security requirements/specifications, documents types and formats, signature standards, and communication protocols.

More details regarding this project and its implementation have not been made public at present. Based on the technical project, the AISS applied for the funding by means of the Structural Funds. Further to the approval of the funding, the project will become public and will be started.

As mentioned above, the service provider will deliver its electronic statements through the Electronic PSC, using its private profile. The same private profile will be also used for correspondence or for receiving electronic documents from the administrations.
28.4 Assessment – Plans, progress and proposals for further harmonisation

28.4.1 Current plans and progress in the implementation of the Services Directive

As mentioned above, several steps were taken in view of the implementation of the Services Directive. The national primary legislation is in a final stage, as the draft of the Ordinance regarding the implementation of the Services Directive is available for public debate and expected to be issued in January 2009.

The technical project regarding the implementation of the Electronic PSC has already been elaborated, and will be implemented further to the issuance of the above-mentioned Ordinance and to the approval of the funding.

The e-government online services were an important experience with regard to the use and issuance of electronic documents. However, as the concept of Electronic PSC is considerably wider, covering a large number of authorities involved and of the services provided through the Electronic PSC, the implementation process is expected to be rather difficult and long term.

28.4.2 Suggestions for further European support initiatives

There are some issues with regard to the implementation of the Directive where European initiatives and support will be highly appreciated in order to facilitate such process, for example reaching an agreement on common document formats for cross border usage.

The Service Directive refers to several common documents that have a standard format mainly including the same content. It is to be determined whether the standardization will regard not only the format of the documents, but also the content of the documents which will be used by the Member States.

Therefore, standardization at an European level would be advisable and necessary for certain types of documents or requests. However, harmonisation will be a difficult step, and will imply long term efforts, as the legislation and requirements of each Member State may differ, and it is not yet clear how such standardization may be accomplished.

The PKI interoperability is a prerequisite for the implementation of the Service Directive at a national level, however there remain issues to be clarified such as the validation of the electronic signature certificate, and the trust lists for the validation of the electronic signatures.
As the interoperability at an EU level e.g. EIF, is considered a must, given the relations between the Electronic PSCs from different Member States, any European initiative, support and cooperation would also be useful.
29 Slovakia

29.1 General framework for electronic documents in eGovernment applications

29.1.1 Electronic documents in eGovernment applications

The basis of legal framework of e-Government is formed mainly by Law on Information Systems of Public Administration. Besides this very general and concise act Slovakia does not have a generic framework related on the very specific issue of electronic documents in eGovernment applications in general. While a relatively large number of eGovernment applications are available to the public, they are regulated and implemented on an ad hoc basis. The problems of e-Government focusing on e-documents will have to be regulated by the act on electronic public administration (eGovernment Act) and by the act on registers of public administration that should be prepared by 2010.

Slovakia has very specific secondary legislation to eSignature Act regulated the requirements for electronic documents signed by electronic signature and used in eGovernment applications (here called administrative intercourse). eSignature Ordinance differs between commercial and administrative intercourse (administrative intercourse is an electronic communication to and from public authorities). To sign electronic documents by advanced electronic signature only the electronic document formats that do not contain active elements may be used. By qualified electronic signature only prescribed document formats are allowed to be signed. This means that

---


593 “Simple” electronic signature defined in Art. 2.1 Signature Directive was not transposed to Slovak legislation.

594 Art. 9 (3) eSignature Ordinance: “If the electronic document format admits the use of active elements, the electronic document containing these active elements may not be signed by an electronic signature and may not be used in commercial or administrative intercourse.”

595 According to Annex 3 of eSignature Ordinance in administrative intercourse is allowed to use only following document formats: ASCII, Microsoft/Apple Rich Text Format (RTF) version 1.5, Adobe Portable Document Format (PDF) version 1.3 and 1.4, HTML 4.01 as defined in international norm (see www.w3c.org/TR/REC-xml ), S/MIME version 3 as defined in international norm (RFC 2633 S/MIME V3) etc.
for electronic documents signed by advanced or qualified electronic signature is very precise regulation in Slovakia.

Technical requirements (e.g. types and formats of electronic documents, communication protocols etc.) are not defined in “soft law” but in Ordinance of Ministry of Finance on Standards for Information Systems of Public Administration that partially creates the legal basis for the formats of documents allowed to be used in information systems of public administration (this regulates only document formats (text and graphic) used in information systems of public administration and not generally for eGovernment applications as such). This is a very specific regulation stipulated technical standards but passed in the form of law (legal regulation).

Thus, electronic documents are not generally issued to end users or requested from them in the context of eGovernment applications, and this is unlikely to change in the near future. From a Slovak perspective, documents as a whole often constitute an unnecessary intermediate step that can be eliminated from public processes by correctly leveraging electronic resources. The introduction of electronic documents to replace paper ones would then not be an optimal step forward in facilitating the life of end users or in improving administrative efficiency.

29.1.2 Electronic documents for the purposes of the implementation of the Services Directive

In August 2007 Slovak government established about 50 Points of Single Contact - PSC (Jednotné kontaktné miesta – JKM). In spite of the existence of points of single contact established in the Trade register offices the Services Directive was still not been fully implemented. The most significant reason is that the introductory procedure can not be done at a distance by electronic means. The application for a trade licence has to be submitted physically (personally) as a filled out and signed document in a local competent Trade register office. Currently trade registers do not have the e-registry to receive the documents signed electronically. Required accompanying documents (such as an extract from the PenalRecord) may be transmitted through the points of single contact.

Points of single contact significantly simplified the access to a service activity. The application needs to be signed by the applicant or by the person representing the applicant (in case of a legal person) and the documents declaring the fulfilment of general terms are not submitted. In an application the applicant can authorise the Trade register to obtain an extract from Penal Record and fill out his/her name of the health insurance company. Subsequently when the enrolment in the Trade Register is done, the Point of Single Contact makes a registration in a health insurance company, fiscal and VAT registration.

596 Announcement of the Ministry of Finance of the Slovak Republic No. 358/2008 Coll. on Issuance of the Ordinance No. MF/013261/2008-132 on Standards for Information Systems of Public Administration, only Slovak version available: http://www.informatizacia.sk/ext_dok-vynos_a_prilohy/5110c

597 E-registry according to the Ordinance of National Security Authority No.542/2002 Coll.
The application for a trade license has to be submitted physically (personally) or by registered postal mail to local competent Trade Register. The local competency is followed by the residence of the legal person or address of the natural person. In Slovakia the Trade Register is established in every of 8 regions (Bratislava, Nitra, Trenčín, Trnava, Banská Bystrica, Žilina, Prešov, Košice).598

The application form can be downloaded from the website of Ministry of Interior, Section of Public Administration, http://www.civil.gov.sk/p09/p09-02.shtm in DOC or PDF format, printed as a hardcopy, filled out and signed on paper with a handwritten signature.

As mentioned above, the introductory procedure has to be done by service provider on paper signed by handwritten signature and only the subsequently communication between administration (Penal Register, health insurance companies and tax authorities) is provided electronically.

Therefore there are actually no clear and precise plans how to accept electronic documents in cases where this is required (including from other Member States and EEA Countries) and Slovakia similar to other Member States is awaiting what trends are emerging at the national level in other Member States or which European Initiatives will occurred.

Besides the PSCs the Slovak government consider to establish the so called Integrated Service Points – ISP (Integrované obslužné miesta – IOM). Those will be physical offices which typically also will have an on-line presence in the form of a website, in which specialised staff are available to assist service providers in identifying and meeting their obligations. The ISPs will assist service providers in identifying the competent professional organisations, and inform the service providers of any requirements for establishment or for providing services. In that sense, the ISPs will have a function as a gateway between service providers and any professional organisations that they may need to communicate with. Currently there is no recognised Integrated Service Point in Slovakia yet.

The fully implementation of the Services Directive is expected to be done in phases in Slovakia. One part based on establishment of PSCs has been already done (amendment of Trade Register Law focused on transposition of Art. 8 Services Directive).

But the specific legal requirements regarding the document types to be supported, Slovakia is similarly awaiting what trends are emerging at the national level in other Member States and Slovakia has actually no clear and precise plans which document types or formats will be used. Because of lack of legal requirements also the specific technical requirements have not been already defined.

With regard to the status of these plans, currently the required legislative changes are being examined, most notably the noted Amendment of Trade Register Act where the Points of Single Contact were established. Other regulatory changes will be implemented until the end of 2009.

598 The completed list with contact data of regional and district Trade registers is published on a web site of Ministry of Interior, Section of Public Services: http://www.civil.gov.sk/p18/p18-04shtm
29.2 Specific document types

29.2.1 Extracts from commercial registers

As noted above, electronic documents are more and more used by Slovak administrations, but the authentic sources are always much favoured. Commercial register is provided in electronic form and the collection of documents in documentary (in writing) and electronic form. The extracts from commercial register exist currently in dual system. The extracts from commercial records may be acquired in traditional documentary form and since August, 1st, 2007 also in electronic form.

The extract is provided by so called Registry Court (that is a district court in the district of county court).

If the application was received to commercial register in documentary form, the extracts are issued in paper and if in electronic form then the applicant will receive an electronic form of extract. Further will be described only electronic extracts from commercial record.

All of information recorded in Commercial Register is publicly accessible and freely searchable on line. The online system is already freely available through a web interface to any interested party for long years, but the information are not usable for legal purpose and has no legal value.

Since August, 1st, 2007 the Ministry of Justice started to issue also electronic documents (electronic extracts from commercial records) that are usable for legal purposes and are legal binding.

Only the users registered in a governmental portal (Central Portal of Public Administration, http://portal.gov.sk) may acquire the extract. During the registration process the user will be asked for name, surname, the date of birth or birth number. Registration is needed the user account to be created where the extract will be delivered.

After the registration process the user fills the electronic application for extracts from commercial register in (available on Central Portal of Public Administration) and pays the administrative fee. Application is not signed by electronic signature. The fee is 10 SKK/0,33 EUR and in comparison with documentary form of extract (200 SKK/6,64 EUR) very advantageous. Latest after two work days since the registered court noticed the payment of administrative fee (common practice is the it is sent immediately after payment), the extract will be send to the user account establish during the registration on the Central Portal of Public Administration or to the e-mail address stated in application form.


600 Actually there are 8 Registry Courts in Slovakia (District Court Bratislava I, District Court Banská Bystrica, District Court Košice I, District Court Nitra, District Court Prešov, District Court Trenčín, District Court Trenčín, District Court Trenčín, District Court Žilina)

601 http://www.orsr.sk (only Slovak version available)
The extract from commercial register is issued in document format .rtf and signed by qualified electronic signature (XAdES) provided by time stamp. The signing certificates are available on the web site of Ministry of Justice.

The validity of electronic extract can be determined through the freely accessible secure verification application QSign (http://www.ardaco.sk) that may be freely download also on the Central Portal of Public Administration (http://portal.gov.sk). To facilitate the process of validation CRLs are used.

As mentioned above, electronic document in the field of Commercial register exists at this time and mostly for reduction of administrative fee begins to be widely used.

29.2.2 Criminal records

Extracts from the penal register (výpis z registra trestov / odpis z registra trestov) exist in Slovakia, but only in a paper format (for public administration partially also in electronic form). The extract is provided by the General Prosecutor’s Office.

People may apply for the extract from penal register only in paper based form and only paper document can be acquired. The electronic application and electronic extract from penal register exist only in the communication between penal register and investigative institutions (orgány činné v trestnom konaní) and Points of Single Contact.

It should be noted that the main barrier in this respect is not the legal framework, since Slovakia has transposed the Signatures Directive at this point, and the use of electronically signed documents for such purposes would thus be legally possible (barring explicit legal provisions to the contrary, which appear to be rare). However, administrative practice has not yet changed to the point where electronically signed documents are commonly available. It is of course clear that extract from penal register could also be produced in an electronic form, using suitable electronic signature solutions, but the General Prosecutor’s Office has not decided to do it yet.

29.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations, orders or stakeholder bodies. While it is difficult to obtain a complete overview, it does not appear that the extracts issued by such private organisations are commonly issued in a paper form. The legal possibility to do so exists, due to the implementation of the Signatures Directive, but in practice only

---

602 Only the document formats laid down in Annex 2 of the Ordinance of NSA No. 542/2002 Coll. can be signed by qualified electronic signature. Therefore any specific legal framework for extracts has been created for Commercial Register. It was up to Ministry of Justice to choose one of the allowed document formats.
paper documents are commonly issued. In instances where electronic documents are made available to the members of a specific profession, this is typically only done in the form of paper copies, notably PDF scans of the original documents.

Currently, no plans exist to make the use of electronic documents mandatory or to encourage them further. Again, there seems to be little added value in issuing separate documents attesting to this fact.

29.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form. While it would be legally possible to do so under the terms of the eSignature Act, in practice there seems to be no demand for electronic certificates, and so far there are no applications or services that require them, either in the public or private sector. Thus, the only electronic certificates of insurance that are encountered in practice are unsigned scanned documents (typically in pdf or tiff formats), which are occasionally used in cases where originals are not required.

Currently, no plans exist to make the use of electronic certificates of insurance mandatory or to encourage them further. For the purposes of Slovak PSCs, the emphasis is mostly on ensuring that original documents are no longer requested unless this is absolutely necessary, in compliance with the administrative simplification obligations of the Directive.

29.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications: generally, these are private and public sector issued documents for which only paper originals are available and actually there are no plans to issue such documents in electronic form. The most significant reason is a lack of infrastructure, insufficient familiarity with the technology and the legal possibilities, or an unwillingness to update procedures that have ostensibly worked well in the past. While electronic copies might occasionally be presented in the form of unsigned scans, this is merely a matter of convenience and this would not present the legal binding document. No specific rules or framework exist for electronic proofs of qualification beyond the general eSignatures Act, and no plans have been proposed to encourage or mandate their uptake.

In general there is a lack of legislation regulating the conversion of paper documents to legal binding electronic documents.

29.2.6 Statements from the service provider

Statements made by the service provider himself will likely be integrated into the websites of the PSC (most probably as the web forms to be completed and signed). It is not yet clear which requirements will be imposed on such statements, beyond the comments made above: in all likelihood, a limited number of signature solutions will be supported in cases where signatures will be required.

Actually the Commission for Standardisation at the Ministry of Finance decided to standardise a format of a certain forms. But it is now unclear, if also the statement from the service provider will have the standardised electronic form. And also the delivery solution of those statements is not stipulated (when signature solution will be supported, there are very strict requirement that have to be meet).

However, this is not a certainty yet, as it depends to some extent on European developments in the near future.

29.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

29.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As was noted above in the explanation of the tasks of PSCs, the introductory procedure has to be done physically what means that the application needs to be signed, but subsequently the documents declaring the fulfilment of general terms are not submitted. In an application the applicant (service provider) can authorise the PSCs (Trade Register office) to obtain an extract from criminal record and fill out his/her name of the health insurance company. Subsequently when the enrolment in the Trade Register is done, the PSC makes a registration in a health insurance company, fiscal and VAT registration.

With regard to the actual communication between the PSCs and these administrations and/or organisations, it is currently being examined how these can be simplified and modernised, to ensure that the service provider will no longer have to correspond with any other entity than the PSC. Service providers will provide any needed documentation to the PSC, who will then process this information in accordance with the procedures that have been defined for each specific service type.

With regard to interaction with Penal Register, the PSC receives from the service provider the application containing his personal data essential for obtaining of extract from Penal Register. The communication between Penal Register and PSC is pursued through the governmental network.
(Govnet) using the encrypted tunnel. The outputs (extracts from Penal Register) are delivered to PSCs as unsigned documents.

With regard to interaction with health insurance companies, the electronic communication is encrypted by PGP, provided without usage of qualified electronic signature and delivering through the simple e-mails. Information systems (CEZIR) sent the requests once a day and health insurance companies deliver their response also once a day.

With regard to interaction with tax authorities, the communication is provided through the governmental network (Govnet). The tax authorities on the basis of request from PSC deliver back to the PSCs the signed document (fiscal or VAT registration statement). During the full-automated signature procedure are used the tools of Central Portal of Public Administration (in particular e-registry and time stamp services).

As noted above, there are already delivery mechanisms in place with technical solution described above, but there is no uniform delivery solution at the national level and the public authorities use the ad hoc individual delivery mechanism. To implement any kind of uniform delivery mechanism at national level, the current framework needs to be changed.

29.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Currently, about 50 Points of Single Contact – PSC (Jednotné kontaktné miesta – JKM) have their physical establishments across the Slovak territory. In spite of the physical existence of PSCs established in the Trade Register offices the Services Directive was still not been fully implemented. The most significant reason is that the introductory procedure can not be done at a distance by electronic means and the application for a trade licence has to be submitted physically (personally) as a filled out and signed document in a local competent Trade register Also the websites are currently mostly informative (including only the forms for downloading) and do not offer possibilities for direct interaction with the PSCs; as such, they cannot currently be considered to be PSCs.

Besides the PSCs the Slovak government considered in the strategic document National Strategy for Informatisation of Society to establish the so called Integrated Service Points (Itegrované obslužné miesta – IOM), where the employees of IOM will assist to citizens and will intermediate between e-services and citizens. The physical establishments of the IOMs will remain in the future, to ensure that service providers can use the channel of communication which they prefer.

Actually, there are no uniform delivery solution at the national level and any solution for delivering of documents from service providers to PSCs exists. Since there is impossible to submit the documents from the service providers to PSCs in electronic form and the introductory procedure has to be done physically, also any individual electronic delivery mechanism is in place. To regulate the delivery mechanism in the future, we need to change our current framework (in particular to laid down the moment of delivery, because from this moment follows the flow of legal periods, further the response time requirements etc.).
With regard to communication with the service provider, no specific decisions have been made at this point yet. However, it seems likely that at an initial stage simple e-mail communication or a similarly accessible technology will be chosen. More complicated and/or highly secured solutions can be considered in the longer term.

When specific electronic documents (such as authorisations or licenses) must be delivered to the service provider, also no specific decisions have been made at this point yet.

29.4 Assessment – Plans, progress and proposals for further harmonisation

29.4.1 Current plans and progress in the implementation of the Services Directive

The Trades Act was substantially amended in August 2007. On the basis of this amendment about 50 Points of Single Contact (Jednotné kontaktné miesta – JKM) were established. Points of single contact significantly simplified the access to a service activity, but in current stage are not based on a principle of a website portal. In spite of the existence of points of single contact in the trade registers the introductory procedure can not be done at a distance by electronic means. The application for a trade licence can not be submitted electronically signed by electronic signature. There is not a legal but technical barrier, because the trade registers do not have the e-registry and are not able to receive the documents signed electronically. The requested accompanying documents (such as an extract from the penal register) may be transmitted through the points of single contact. In an application the applicant can authorise the trade register to obtain an extract from the judicial record from Penalty Register and fill out his/her health insurance company. Subsequently when the enrolment in the Trade register is done, the point of single contact makes a registration in a health insurance company, fiscal and VAT registration

Until the e-signature in trade register will be not implemented and e-registry will not be established the fully electronic process will be not possible and the foreign service providers will not be able to identify them and fulfill specific requirements at a distance from their national countries.

For the future is the enlargement of functionality of points of single contact expected. The plan is, that not only registration in a trade register will be available service in it, but also the process of enrolment in a Commercial Register will be added (which is currently available as a independent service not using the points of single contact). Also the addition of other self employment economic activities (not only on the basis of trade licence) is planned.

---

604 E-registry according to the Ordinance of National Security Authority No.542/2002 Coll.
29.4.2 Suggestions for further European support initiatives

Given the Slovak emphasis on authentic sources and web services rather than electronic documents, the creation and expansion of trusted networks to exchange authentic information between mandated parties would seem to be a favoured option. However, as an interim step, Slovakia would also welcome further harmonisation of existing electronic documents. From a technical perspective, the Slovak infrastructure would be able to accommodate most widespread standards, so that there is no specific preference in this regard. Similarly, if this would be necessary and beneficial, it would be possible for Slovak administrations to deliver electronic documents as well via web services or through the so called e-registries already established in many administration bodies and available also on Central Portal of Public Administration.

With regard to electronic signatures, in cases where signatures will be required both types of electronic signatures regulated by Slovak law (advanced and qualified electronic signature) may be used. In principle, the Slovak approach is envisaged to support also a limited number of certification service providers of other Member States, but the national requirements from each Member States for service providers are very different. Therefore the envisaged model of a trusted list (but not only a common template of trusted list) is very much invited. However, to ensure that implementation efforts are kept manageable, this list should be kept limited in scope (15-20 CSPs are currently envisaged).

But, before any kind of European initiatives will come in place, the conclusions of IDABC Preliminary study on mutual recognition of eSignatures for eGovernment applications cannot be put out of mind. Findings of the Study, mostly that public sector principle (Art. 3.7 Signature Directive) and voluntary accreditation scheme were misunderstood by national governments are very significant. It is noteworthy that the Signature Directive prohibits the “creation of obstacles to cross-border services for citizens”, but this was not interpreted in a strict sense. It is clear that there is a divergence in interpretation and implementation of public sector provision and in voluntary accreditation principle in most of the Members States. It is interrogative if only the correct implementation of Signature Directive in national countries would not be sufficient and would not return the cross border use of electronic signature to European Countries (at least on the legal level). The European Union should enforce the correct implementation of Signature Directive, should weight the consequences and give back the original sense and interpretation of Directive. Since a number of Member States are still deploying their electronic signature infrastructures this can present a problem for those countries. This is the key point that has to be kept in mind before any further European initiative will appear.

Also the cross border use of electronic signatures within a PSC is subject to all the usual difficulties in cross border e-government applications which are as of yet unsolved and which have been described very recently in great detail in the IDABC Preliminary study on mutual recognition of eSignatures for eGovernment applications. The most significant problems are the lack of means of verifying the validity of foreign signatures, further that the recipient cannot determine the legal value of the signature as being a qualified signature or otherwise etc. But most of the cross-border problems follows from the noted issue of incorrect implementation of Signature Directive and creation of cross border obstacles in usage of e-signatures.

Most of the problems identified during the implementation of Art. 8 Services Directive are more or less limited to eSignature problems and has their basis in incorrect implementation of eSignature Directive. Therefore before any further European initiative would come in place it should be considered if the enforcement of the correct implementation of eSignature Directive in the Member States and possible infringement would not be a way to solve most of the problems.
30 Slovenia

30.1 General framework for electronic documents in eGovernment applications

30.1.1 Electronic documents in eGovernment applications

Slovenia does not have a general framework related to electronic documents in eGovernment applications. Notwithstanding the fact that a relatively large number of eGovernment applications are available to the public, they are regulated and implemented on an ad hoc basis.

A general observation is that the applications do not rely on electronic documents themselves. Electronic documents are mostly understood as a direct replacement of existing “paper” documents.

Slovene legislation also doesn’t have a special definition of the term electronic document; however the Electronic Commerce and Electronic Signature Act provides the definition of data in electronic form (Article 2, indent 1). Accordingly data in electronic form are data which are electronically designed, stored, sent, received or exchangeable. This definition clearly applies also to electronic documents, which could be described as a subgroup of data in electronic form, having some additional attributes in design.

As far as the validity of electronic documents in general are concerned Article 4 of the Electronic Commerce and Electronic Signature Act explicitly provides that data in electronic form may not be declared invalid or lacking in evidential value solely because they are in electronic form. Another provision in this respect is provided by paragraph 1 of Article 13 of the Electronic Commerce and Electronic Signature Act which states that where the law or other regulation requires a written form in order for to document to be legally valid, an electronic form shall be considered equivalent to the written form if the data in electronic form are accessible and appropriate for later use. There is no additional formal requirement to accessibility and suitability for later use as far as the document type is concerned.

Restrictions to the acceptability of electronic documents are provided in Paragraph 2 Article 13, as certain contracts are excluded from valid formation in electronic form. This restriction covers contracts on legal transactions transferring ownership rights to real estate or establishing other material rights to real estate, testamentary transactions, contracts arranging property relations between spouses, contracts disposing of the assets of persons declared legally incapacitated, contracts on the handover and distribution of assets for life, endowment contracts and agreements on renunciation of inheritance, promises of gifts and gift contracts in the event of death, other legal transactions which

606  http://e-uprava.gov.si/e-uprava/
the law stipulates must be concluded in the form of a notarised record. All of the above mentioned contracts require according to the law at least the written form in most cases, and also an additional formal intervention of a public body (e.g. Notary) for some documents.

As certain documents will need to be signed, rules on electronic signature also have to be observed. The legal basis for signature requirements is provided by Article 15 of the Electronic Commerce and Electronic Signature Act stating that secure electronic signatures certified by a qualified certificate shall with regard to data in electronic form be equivalent to a hand written signature, and shall have the same validity and evidential value. This provision applies to natural as well as legal persons, and is thus applicable also in eGovernment applications.

Notwithstanding the mentioned restrictions above the definition of electronic documents emphasizes almost all electronic documents used in practice and is, together with the notion of eSignature also applicable in eGovernment applications. Accordingly no legal barriers for the validity of almost any document, fulfilling the criteria of being accessible and appropriate (and also duly signed by a competent individual) for later use can be identified.

Although several applications were established especially for governmental “back office” solutions, (and bearing in mind that no legal barriers as such exist) electronic documents are in practice still not seen as replacements for physical documents, but merely as means of faster communication. An interesting observation in this respect is that in the time of the Slovene presidency (Jan-Jun 2008) it even took a special government declaration (commitment) not to use postal services for government internal communications as an effort to reduce emerging costs. This well describes the still prevailing practice of relying on physical documents.

30.1.2 Electronic documents for the purposes of the implementation of the Services Directive

Though a first draft implementation Act for the services directive is due to be presented in December 2008 it is not foreseen that it will cover the issue of electronic documents. This is somewhat logical as the definition described above is perfectly applicable also for the eServices directive.

However in the process of the implementation of the eServices directive several questions may arise.

Firstly as the Ministry of the economy will most likely be the focal point (PSC) of communications according to the eServices directive any procedure according to the Services Directive will per definitionem be an administrative procedure. Consequently relevant provisions of the General Administrative Procedure Act will apply if not provided otherwise, as subsidiary use is mandatory to any administrative procedure (hereby we presume that no special framework will apply).

608 http://zakonodaja.gov.si/rpsi/r03/predpis_ZAKO1603.html
To this end it must be noted that the General Administrative Procedure Act provides a very clear legal basis for electronic administrative procedures which are strictly formal. However in most cases a written form with an autographic signature is sufficient to file almost any application. As the framework for their equivalence is already provided by the Electronic Commerce and Electronic Signature Act (described above), a reference to its provisions was the most logical solution.

In this respect it should be clearly stated that a complex general legal framework for electronic communication with public administrations already exists. Accordingly all applications can be legally filed in electronic form (Article 63, paragraph 2) notwithstanding the fact an electronic application exist or not. As an application requires the signature of the applicant in this respect the relevant provisions of the Electronic Commerce and Electronic Signature Act will apply; to this end a secure electronic signatures certified by a qualified certificate must be used. Such an electronic application is processed by the central governmental information system for filing, notifying and handing over, which automatically sends out a confirmation of receipt to the applicant. Acceptance and processing of electronic documents and participation in the central information system is according to the provisions of Article 63, paragraph 4 mandatory for all administration bodies within at the level of central government and other public authority holders at the central governmental level. A special written authorisation for participating in the information system can be issued also to self-government authorities at the local level and to holders of other public authorisations. Issues of filing, issuance and receiving of electronic documents are also all well regulated by the General Administrative Procedure Act.

Further the General Administrative Procedure Act contains also provisions (Article 139) aiming at the facilitation of exchange of information between public bodies in processing application. Accordingly a public body processing an application may not require documents from the applicants if those can be obtained from publicly accessible registers of other public bodies or, in case of non-public registers, if the applicant explicitly authorises the public body processing his application to such access.

The described observations are crucial in terms of the implementation of the eServices directive as it represents a legal basis for mandatory acceptance of electronic documents by the different stakeholders but also for their issuance in electronic form as well as their mutual electronic correspondence.

The second crucial observation to be made in terms of the implementation of the eServices directive is the scope of regulated professions. A list of regulated professions is provided by the Ministry of labour, family and social affairs:


Accordingly today in Slovenia there are more than 300 regulated professions, regulated by different sector specific legislation. Although some of them may be excluded from the scope of the Services directive (like e.g. healthcare services) the list nevertheless provides an illustration on the overall scope of necessary measures for the implementation of the Directive which is in fact enormous.

Notwithstanding different Ministries being stated in the list as being competent for regulatory issues, the Ministries are in the majority of cases not holders of professional registers themselves. Competent
authorities for procedures and formalities relating to access to a service activity covered by the Directive and to the exercise thereof will in practice most likely be different professional bodies acting upon authorization provided by law. Some services (e.g. opticians) require a permit prior to establishment, whereas others don't. Notwithstanding that in the majority of services this will not apply, it doubtlessly has some influence on the list of activities as they do not necessarily follow the same procedures.

30.2 Specific document types

30.2.1 Extracts from commercial registers

As noted above, electronic documents are not normally used in Slovenia and the re-use of authentic sources is much favoured; commercial registers are an example.

All key information related to economically active independent entities (companies, institutes, entrepreneurs etc.) is electronically processed and accessible in the Slovenian Business register (iPRS) managed by AJPES - Agency of the Republic of Slovenia for Public Legal Records and Related Services (http://www.ajpes.si). Basic information about these entities includes:

- Full name and legal form;
- Unique enterprise number;
- Tax or VAT ID number
- Seat of establishment and date of establishment;
- Company bodies and their members
- Management details,
- Basic Legal information, liability, ongoing (not yet registered) registry procedures, general assembly protocols and decisions

All of this information is publicly accessible and freely searchable on line upon prior registration (which is also free). Data can be accessed by entering the search criteria in one or more fields, or by selecting the search criterion from the drop-down menu. The most common search is an updated registry extract.

From the beginning of 2008, all registry entries must mandatorily be provided in an electronic format (.pdf or .tiff), and prior (paper) entries are being digitised.

After the publication of the Business register on the internet in electronic form, different authorities will no longer require extracts, as the relevant establishment data are accessible directly and updated via the internet; however this only holds true for Slovene established entities. Observing Article 139 of the general administrative procedure Act, it is even questionable if Slovene administrations still have the possibility of requesting extracts as they are obliged to acquire public registry extracts by themselves.
30.2.2 Criminal records

The criminal record is managed by the Ministry of Justice, separately for natural and legal persons. An individual demonstrates his status with an extract of the judicial record (also referred to as the certificate of non conviction). This certificate ascertains that a natural or legal person was or was not found guilty for a crime by a definite ruling. The certificate is provided by the Ministry of justice at the cost of 1,06€; in practice it is submitted on paper the day after an application is submitted.

For now no electronic document – attestation – itself exists, however the request for an extract can be submitted electronically in several ways, which are accessible on: http://www.mp.gov.si/si/potrdila_in_obrazci/

Basically there are two ways for filing a request, both available at no cost. The first is a model document which can be downloaded, signed and filed manually, whilst the second is an application, which can be accessed using a qualified electronic certificate (PKI system). Hereby certain basic identification data of the applicant must be submitted.

The certificate itself however is always a physical (paper) document and no such electronic document exists. It is manually signed by the Minister and sent by post to the applicant.

As this is an administrative procedure, observations made on electronic processing of the General administrative procedure Act and the notion of the electronic document can be referred to. Accordingly no direct legal barriers on the acceptance of electronic certificates of non-conviction itself can be identified, and thus issuance/acceptance is in theory already possible.

A separate record is kept also for minor offences (misdemeanors), which can be accessed very much in the same way.

30.2.3 Extracts from professional registers

Professional registers are typically managed by private entities, such as professional organisations, orders or stakeholder bodies, however as already explained above they can also be held by different ministries. To our knowledge for now there are no applications enabling the issuance of electronic attestations from these registers.

Bearing in mind that the definition of electronic document under Slovene law is very broad the same observations on their validity as above can be made; thus also scans of paper origins could be acceptable (it is however questionable how their validity in this case could be determined).
30.2.4 Certificates of insurance

Certificates of insurance are not issued in an electronic form, and in practice they are required only in paper form. While it would be legally possible to create and use electronic certificates under the terms of the E-commerce and E-signatures Act, in practice there seems to be no demand for electronic certificates, and so far there are no applications or services that require them, either in the public or private sector. As certificates of insurance refer to a certain point to the financial status of the subject, there is some additional reluctance to accept them in any other form than the paper original.

30.2.5 Proofs of qualifications

As with extracts from professional registers, proofs of qualifications are also in majority issued by private entities, mandated to do so by law, and for which only paper originals are available. Thus the same observations as above (under extracts of professional registers) can be made.

30.2.6 Statements from the service provider

Statements made by the service provider are typical expressions of will. Thus the general principles of non-discrimination of the electronic form can be applied. To this end the very same observations can be made as on the general validity of the electronic form. This is recognized by law as valid if it fulfills the criteria of accessibility and suitability for later use.

At this time no information on the use of statements in the implementation of the Services Directive can be provided.

However it is very likely that any statements of the service provider could be integrated into the web application (or part of it) used in order to implement Article 8 of the Services Directive as there are no legal barriers which would hinder the validity of such statements. To this end if no additional formal requirement is needed even “click-use” statements would be legally sufficient, provided an according back-office solution is applied.
30.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

30.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As already stated, a draft implementation law is still to be presented, and thus no relevant information can be provided at this time. Generally, it is unlikely that the implementation Act itself will contain any provisions, regulating back office solutions at a technical level. Given the scope of public bodies involved this is highly understandable.

For now the only more or less definite decision is that the organisation of the PSC will be within the competences of the Ministry of the economy, whereas technical choices fall within the competences of the Ministry for public administration.

Notwithstanding future solutions aiming at the implementation of Article 8 of the Services directive (as the key provision de facto requiring back-office communication solutions), at least for the legal part of the implementation work the relevant provisions of the General Administrative Procedure Act are completely applicable. As any procedure of the PSC will be an administrative procedure, its provisions are fully applicable not only on the part of the PSC but also on the part of its correspondents. As far as the current legislative situation is concerned, following Article 63, paragraph 4 of this act, participation in the central governmental information system is already mandatory for all administration bodies within at the level of central government and other public authority holders at central governmental level, whereas for others only an authorisation for participating in the information system must be provided. It is perfectly possible that a general provision in the implementation Act is sufficient, covering all possible public bodies. As the exchange of information between public bodies in processing an application is also regulated (Article 139 of the General Administrative Procedure Act), the main legislative issues could already be resolved.

However, legislative provisions will likely prove insufficient in order to ensure full implementation of the Directive. Baring in mind that currently there are over 300 regulated professions in Slovenia, resulting in almost as many different procedures it is doubtful whether a general solution is at all possible. To this end a more realistic suggestion could be that in practice a detailed case to case approach will be needed.
30.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

As a draft implementation law is still to be presented no relevant information can be provided at this time. The current plan of a front office solution suggest a website/application, organisational within the Ministry of the Economy (which will also function as PSC) in a legal form yet to be determined, with technical support of the Ministry for public administration.

30.4 Assessment – Plans, progress and proposals for further harmonisation

30.4.1 Current plans and progress in the implementation of the Services Directive

According to information from the Ministry of the Economy the implementation law of the services Directive is currently in preparation and should also shortly be presented to the public. Following the governmental schedule this should already be in December 2008, it is however doubtful that this deadline will be met (due to the parliament elections this fall and consequent change of government).

Nevertheless some outlines of the future legislative framework can already be identified. As stated in the overview the Ministry of the economy is likely to perform the PSC’s tasks. Another key observation in view of the directive’s implementation is that the implementation Act prepared by the ministry of the economy will be a general framework law and thus will not directly regulate the sector specific implications of the Directive.

As far as other issues on progress are concerned we refer to other observations made in the report.

30.4.2 Suggestions for further European support initiatives

The described implementation approach is most logical and in view of the overall scope of regulated professions under Slovenian law perhaps the only possible legislative solution. However the major problem will still remain the practical implementation to any individual service covered by the directive, as at least for a certain period of time some procedural and also formal questions may arise which may lead to a redefinition of the procedures.

In terms of practical implementation the administrative legislative framework can be regarded as already in place but also certain key applications, like the on-line establishment of companies and electronic access to the company/business register are already applicable and in use. However in view of ca. 300 regulated professions with divergent procedural requirements the existence of some
technological solutions can hardly be regarded as sufficient to comply with the requirement of Article 8 of the Services directive. To this end EU initiatives facilitating and/or exploring already working solutions could prove useful.

However this is only the Slovene internal part of the implementation in which we presume the issues related to the identification and authentication of EU applicants (service providers) will already be resolved. In fact this may prove to be a major problem. Notwithstanding the mutual recognition of e-Signatures deriving from Directive 1999/93 its practical implementation remained limited due to technical possibilities of the very application. This may be problematic also in this case. In our opinion two strategic possibilities for EU initiatives could be suggested:

1. Harmonisation of authentication technology at PSC level (at least) or
2. Additional or parallel identification procedures from PSC to PSC whereby the PSC of the applicant could certify his identification to the other PSC.
31 Spain

31.1 General framework for electronic documents in eGovernment applications

31.1.1 Legal framework of electronic documents


Among its definitions, the eSignature Law, after a modification that took place in 2007, refers to the electronic document (Article 3, paragr. 4 to 7), as “electronic information of whatever nature, drawn up on electronic medium according to a specific format, and liable to identification and individual processing”.

Electronic documents will be medium of:

- **Public documents** eSigned by public officers with faculties to Law as legal authorities (e.g. notary public, county clerk or other administrative officers) to authenticate documents, within the limits of the rules applicable to their public functions.

- **Administrative documents**: those issued and eSigned by public officers or public employees in the performance of their public duties, within the limits of the rules applicable to their public functions.

- **Private documents**.

Any of those three eDocuments will have the value and legal effectiveness corresponding to their respective nature, in accordance to the rules applicable to them. And the medium in which data are eSigned will be admissible as documentary evidence within a trial.

Finally, the Spanish eSignature Law allows enterprises to apply for electronic corporate signatures via their legal representatives, so as to use them in their common relations with the Public Administrations (theoretically at all levels: state, regional and local), or in their commercial transactions, as well as in the normal contractual relationships of the company. Examples of the common use of corporate electronic signatures are tax declarations and the filing of annual accounts at the Corporate Registry.

---

which can be made in digital format if they are signed with a recognized (qualified) electronic signature.

31.1.2 Electronic documents in eGovernment applications

In Spain since 2004 it has been notably intensified the implementation of common services and infrastructures. Among others, the issue of the electronic ID card, the development of a common platform dedicated to validate digital certificates (@firma), the draft of a Plan of digital services related to the eID card, the development and spread of an inter-administrative communications network (SARA Network) to which most of the regional administrations and many local administrations are already connected; the creation, for the first time, of intermediary services that allow to eliminate the request of ID card photocopies or certificates of registration on the electoral roll within the administrative transactions; the creation of an integral network of citizens service department (Red 060 – Network 060) that includes a website of general access to all on-line eGovernment services, a unified telephone number and a network of offices, among others.

The Ministry of Public Administrations has compiled the principal electronic services provided by the State Administration with major impact for citizens and companies, distinguishing more than 325 services, of which one half were addressed to citizens and the other half to companies. 50% of them have reached a high level of on-line transaction by using the eID card or other digital certificate identifying the user, so as to avoid the presence phase of the procedure.\footnote{Data obtained from explanation given on the Strategic Plan of development of Law 11/2007 (see more references below)


Specific requirements with regard to electronic signatures are reflected in the Administration eSignature Policy, included in the framework of national interoperability.

\footnote{Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos}
For documents provided by citizens the future Royal Decree recommends to apply the eSignature in the cases when it is considered necessary.

The eSignature Policy recommends the eSignature formats XADES and CADES; and the abovementioned future Nacional Scheme of Interoperability will include guidelines for documents formats, recommending the use of open formats (e.g. ISO 32000 PDF, ISO 26300 ODF, ISO 24517 PDF(E)) and specially PDFA (ISO 19005), thinking on a long term conservation.

Regarding data in applications, it will be necessary to create XML files that may be managed outside its original application if they are necessary. This may also apply to the metadata that will accompany each electronic document.

### 31.1.3 Electronic documents for the purposes of the implementation of the Services Directive

Law 11/2007 was approved in June 2007, being the rule that, for the first time, spread the citizens’ right to make transactions with the Spanish public administrations by electronic means. Following to the Services Directive, the established term for right to be effective is 31st December 2009: by then all public transactions will have to be electronically accessible.

This Law foresees the conditions for the electronic provision of these services, supplying the lack of regulation on certain aspects of the electronic relations between citizens and administrations, thus eliminating the legal barriers for the complete development of the eGovernment in Spain.

Moreover, Law 11/2007 collects under one text all scattered existing rules on eGovernment and consolidates a common regime of guarantees and citizens’ rights, adjusts the regulation to the technological reality, and guarantees the interoperability of the technological solutions developed by the different Administrations.

The Spanish administration will accept electronic documents, even if they are issued in other Member States and EEA Countries, in cases where this is required, following the current regulation and the European agreements (if they are included in the European interoperability framework). In this sense, Law 11/2007 gives details (article 43) on the communication network among the Spanish public administrations at all levels, state, regional and local -including their consortiums or cooperation entities incorporated for these purposes-, will adopt the necessary measures to interconnect their networks, creating thus a communication network what will enable the exchange of information and services among them, and their interconnection with the networks of the EU Institutions and the member states.

Besides, to this regard, in December 2007 the Spanish Government announced the “Plan of Development of Law 11/07 of electronic access”\(^6\)\(^{12}\), which, among others includes common infrastructures and services, and more specifically:

---

\(^6\)\(^{12}\) “Plan de desarrollo de la Ley para el acceso electrónico a los Servicios Públicos” Full information on the Action Plan and Strategic Plan, and actions per Ministry, available at [http://www.csi.map.es/csi/nuevo/administracion_electronica_7.htm](http://www.csi.map.es/csi/nuevo/administracion_electronica_7.htm) See more references to these Plans below.
• In order to develop new eGovernment services it will be given to all public Administrations a joint offer of infrastructures and common services that will provide the start up of these services and the interoperability among them (the use of these services will be offered in a voluntary basis, and according to the agreements signed among Regional and State organisms).

• A high-speed and highly available communications network will be provided to the public Administrations, extending the performance of the current network “Sara”.

• In order to promote the development of needed software solutions, guarantee the interoperability and reduce costs and implementation terms.

Nevertheless, there are no specific legal requirements for the implementation of the Services Directive. Concerning the technical requirements, it will be applied the ones established in the eSignature Policy and in the Interoperability national scheme: the eSignature Policy is published for its consultation by any administration, and it is still pending the publication of the Interoperability Scheme, foreseen for the first quarter of 2009 (as well as the publication of the RD developing Law 11/2007). The eSignature formats that will be employed for PSCs, according to the eSignature Policy, follow the ones that are being discussed now in the Technical Working Groups for the implementation of the Services Directive so that the eSignatures will be interoperable at European level.

The Interoperability National Scheme will comprise a number of criteria and recommendations in the fields of security, conservation and standardization of information, formats and applications that have to be taken into account by the public administrations when they take technologic decisions that will guarantee the interoperability.

### 31.2 Specific document types

#### 31.2.1 Extracts from commercial registers

Spain has a Central commercial register, common to all the Spanish territory and provincial registers, where companies will be registered according to their address (location).

At present, at the Central Commercial Register (www.rmc.es) it is only accessible on-line the request of a corporate name, which does not require the use of an eSignature; it is only necessary to provide the ID card number together with a VISA card number, in order to pay the certificate, which is physically issued, handwritten signed and delivered in hand or sent by ordinary mail to the interested person. This also applies to on-line requests of informative simple notes containing all or an extract of the content of the Register (corresponding to a registered company); the note is issued, signed and sealed by the official in charge of the Register, mentioning the number of pages and date.

In case of voluntary modification of the corporate name, the request can also be made electronically: on-line through the abovementioned website. Or through the Notary that formalizes the public deed, by using the e-notario platform; in this case, the certificate will sent to that Notary with the recognised (qualified) eSignature of the registrar entitled of the Central Corporate Register.
The on-line processing system of CIRCE\textsuperscript{613} (Information center and network of company’s incorporation) is a computer service of electronic files’ processing that will enable the exchange of all documentation necessary for the incorporation of companies.

At present all Commercial Registers included in the CIRCE Network are ready to qualify and inscribe deeds of incorporation corresponding to “limited new enterprises” as well as all limited companies. Therefore, at the provincial register it is possible to electronically inscribe a company. The Registrars association provides digital certificates to registrars for their eSignature, which is validated through the validation platform @firma, connected to all authorised providers by methods CLT or OCSP (See more info at the PSC paragraph).

All transactions for the on-line incorporation of a company are available at http://www.circe.es/Circe_Publico_Web/Articulo.aspx?titulo=que_es (and more references below).

### 31.2.2 Criminal records

The certificate of criminal records is issued in Spain by the Ministry of Justice. It is not provided electronically because at present it is printed in stamped paper.

The application of this type of certificate may be presented in person or via traditional mail (full information available at:


It is among the procedures non adjusted to the provisions of Law 11/2007. The full updated list is accessible at:


The only thing admitted on-line regarding this certificate is the payment of the application tax, which requires the use of a digital certificate by the interested person.

\textsuperscript{613} CIRCE: Centro de Información y Red de Creación de Empresas (Information Center and Network of Companies Incorporation)
31.2.3 Extracts from professional registers

In Spain, in general terms, the so-called “Colegios profesionales” (Official Professional Associations) are private professional institutions where students that have obtained certain academic degrees (traditionally, Medicine, Pharmacy, Engineering or Law), or official qualifications should be registered in order to legally exercise their profession in Spain. This type of registers exists in many cases at regional level, as the Spanish Regions have competence on the regulation of professional associations and qualified or graduated professions.

But there are also the so-called “Asociaciones Profesionales” (non-official Professional Associations) where inscription is not compulsory in order to legally exercise a profession.

The legal framework of the “Colegios Profesionales” will be subject to review and modification so as to be adjusted to the provisions of the Services Directive.

It is difficult to obtain a complete overview, and as a general rule, it seems that the extracts obtained from such private organisations are commonly issued in a paper form, even though the eSignature Law allows the electronic form.

Currently, no plans exist to make the use of electronic documents mandatory or to encourage them further at State level.

31.2.4 Certificates of insurance

As a general rule, certificates of insurance companies in Spain may be applied in an electronic form. Within the public sector, such is the case of MUFACE (insurance company of State civil servants), that offers the possibility to apply and obtain on-line a wide range of certificates: affiliation, health assistance coverage, benefits obtained, beneficiaries included in the affiliation document. See: http://www.map.es/muface/muface/carta_de_servicios/common/Carta_servicios_elctr.pdf

---

614 E.g. Colegio Oficial de Ingenieros de Telecomunicaciones (telecommunication engineers www.coit.es),
616 E.g. of Geologists or Insurance mediators
617 On this particular subject see a recent Report drafted by the Competition National Commission on the professional services sector and professional associations http://www.unionprofesional.com/UserFiles/File/EnProceso/Informe_CNC-(150908.pdf)
It happens the same with the private sector, as Insurance Companies usually have a virtual space\textsuperscript{618} for their clients where they may have access to updated information on their products, modify their contact details or request on copies of the contracts can take place by electronic means but then paper duplicates are sent by ordinary mail.

Currently, no plans exist to make the use of electronic certificates of insurance mandatory or to encourage them further.

31.2.5 Proofs of qualifications

Proofs of qualifications are private / public sector issued documents for which only paper originals are available.

While electronic copies might occasionally be presented in the form of unsigned scans, this is merely a matter of convenience. No specific rules or framework exist for electronic proofs of qualification beyond the general eSignatures Law, and no plans have been proposed to encourage or mandate their uptake.

Nevertheless, regarding the University framework, there are already some cases, as eg. the University of Girona (Catalonia) where some of its members, as well as members of the government body have been provided of recognised (qualified) signature certificates\textsuperscript{619} in the University computing devices, as well as secure computing devices, so that they may operate on-line by secure and effective means. And according to the CRUE\textsuperscript{620} it is accurate to mention that some Spanish universities are already issuing academic electronic certificates which is obviously not the same as the paper-stamped-title issued by the Education Ministry, but proves that the person has studied a carrier; and within the context of the PSC and for certain transactions it may be considered as a proof of qualification.

31.2.6 Statements from the service provider

The tendency will be for service providers to use standardized electronic forms available at the PSC, in order to make their statements. When the eSignature is needed, the system will let him use the forms at the PSC by using any of the methods established by Law 11/2007 (eID card, digital certificate or code).


\textsuperscript{619} Digital Certification Service provided by CESCA (Centre de Supercomputació de Catalunya), through the Entidad de Certificación de Universidades e Investigación (EC-UR)

\textsuperscript{620} CRUE: Conferencia de Rectores de Universidades Españolas (Vice-Chancellors Conference of Spanish Universities) www.crue.org
Then, the delivery of his electronic statement to the PSC (e.g. via a webform, e-mail, Word documents, ...) will depend on the maturity of the competent authority.

The requirements in relation to signatures that these documents need to observe are the ones established in the eSignature Policy.

31.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

Electronic access to the public services will be expanded by creating PSCS and “ventanillas únicas sectoriales” (sectorial PSCs) that will make unnecessary a global knowledge of the State Administration internal structure in order to accede to the required services. These services will be designed according to the needs of citizens and companies.

31.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

PSCs will still be in charge of identifying the appropriate bodies that need to be communicated with on behalf of the service provider.

With regard to the actual communication between the PSCs and these administrations and/or organisations, it is currently being examined how these can be simplified and modernised, to ensure that the service provider will no longer have to correspond with any other entity than the PSCs. Service providers will provide any needed documentation to the PSC, who will then process this information in accordance with the procedures that have been defined for each specific service type.

With regard to interactions with public administrations (such as the registration of enterprises in official databases, VAT registration, registration as an employer, etc.), the PSCs will be able to use web services which are currently being created and expanded at state level. For communications with private organisations, most interactions will not be automated, and the PSC staff will instead contact the competent organisations directly via any appropriate means – which may include e-mail, but also more traditional means such as fax, telephone or even traditional mail – to ensure that the information is processed correctly. This is however a new task for enterprise PSCs, whose legal responsibilities thus far has only included interactions with public authorities.

If service providers of other Member States rely on foreign electronic documentation which is difficult or impossible for the PSC to validate, it is currently foreseen that this information will be validated through the IMI system621.

621 The Internal Market Information System; see http://ec.europa.eu/idabc/en/document/5378/5970
PSCs have already been in operation for quite some time, but they will not provide all the services described above until the required legislative changes have been made.

31.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

The Services Directive requires that the service provider must be able to communicate exclusively with the PSC if he so chooses, and thus not with any other public administrations or private organizations that might be competent to make decisions related to the service activity. In Spain this will depend on the maturity of the competent authority: the delivery may take place by e-mail or through a virtual site at the service provider’s disposal.

Ventanilla única empresarial (Enterprise PSC)

The Enterprise PSC\(^{622}\) aims to support enterprising in the incorporation of new companies, by rendering integrated advising services on processing and business.

The Enterprise PSC provides with:

- Presence advising centers.
- The Internet Portal of the Virtual Enterprise PSC\(^{623}\), offering general information on companies’ incorporation, a tool of personalized guidance, on the transactions of each business project, as well as an individual follow-up system of all the steps followed in the company’s incorporation process.

This is a joint initiative of all Spanish public administrations (state, regional and local), together with the Chambers of Commerce.

On-line incorporation of companies (CIRCE)\(^{624}\)

As mentioned above, for the incorporation of a Ltd. Company, an on-line procedure is already available, assisted in offices acting as Points of Advice and Start of Transactions\(^{625}\) (different to the

---

\(^{622}\) See [http://www.ventanillaempresarial.org/menu.htm](http://www.ventanillaempresarial.org/menu.htm)


\(^{625}\) The so-called “Puntos de Asesoramiento e Inicio de Tramitación” (PAIT)
enterprise PSCs, even though apparently the second ones might also assume these tasks); it contributes to avoid unnecessary displacements, reducing timing and costs.

In these offices, professional associations and business organisations are also implied, and their objective is:

- To render presence information and advice services to enterprising in the definition and online transaction of their business initiatives, and during the first years of activity of the Ltd. Company.

- To start the administrative procedure of incorporation through the “Electronic Single Document” (Documento Único Electrónico: DUE\(^{626}\)). The DUE is conceived as an on-line tool that includes all data referred to the Ltd. Company that, according to the current legislation, have to be delivered on-line to public registries and public administrations, in order to get its incorporation and for the accomplishment of all fiscal and Social Security obligations required for the activity start up.

The DUE will contain two categories of data: (1) basic data, legally required in order to start the procedure, as well as those necessary to implement the DUE transaction; (2) data to be added in each phase of the incorporation procedure, by the responsible of the legal registries, the competent public authorities (concerning fiscal and Social security requirements).

Currently, the enterprise PSCs have multiple physical establishments across the Spanish territory, in addition to a single website per sector (but not per establishment). As noted above, the websites currently are mostly informative and offered limited possibilities for direct interaction with the “ventanillas”; as such, they cannot currently be considered to be PSCs.

The physical establishments of these type of PSCs will remain in the future, to ensure that service providers can use the channel of communication which they prefer. However, the web sites will be expanded to ensure that they can be used by the service providers to communicate directly with the PSCs. As noted above, this will require changes both at the legal and at the technical front (by making web services available at the state level which the enterprise kiosks can use). Elements such as response time requirements, use of specific languages, and liability have not yet been reviewed.

With regard to communication with the service provider, no specific decisions have been made at this point yet. However, it seems likely that at an initial stage simple e-mail communication or a similarly accessible technology will be chosen. More complicated and/or highly secured solutions can be considered in the longer term.

When specific electronic documents (such as authorisations or licenses) must be delivered to the service provider, a number of possible solutions are still being considered, and it is not yet clear how this situation would be handled.

---

\(^{626}\) Regulated by Royal Decree 1332/2006, establishing the specifications and conditions for the use of the DUE for the incorporation and start up of Ltd. Companies through the on-line procedure (Real Decreto 1332/2006, de 21 de noviembre, por el que se regulan las especificaciones y condiciones para el empleo del Documento Único Electrónico (DUE) para la constitución y puesta en marcha de sociedades de responsabilidad limitada mediante el sistema de tramitación telemática). Text available at: http://www.circe.es/WebFiles/Images/e/e2/A42119-42121.pdf
31.4 Assessment – Plans, progress and proposals for further harmonisation

31.4.1 Current plans and progress in the implementation of the Services Directive

- At present, as shown in the overview above, Spain already has an advanced infrastructure in place for the implementation of the PSCs (CIRCE system, on-line notifications, enterprise PSCs, the 060 or the eSignatures systems).

Regarding the electronic document, several aspects on interoperability are still being defined regarding the formats, electronic filing (in the National Scheme of Interoperability).

Concerning the eSignature formats, this matter is quite advanced, as there is a national eSignature Policy including the formats and technical characteristics that eSignatures should incorporate in order to be interoperable. The already defined formats (XADES and CADES) are absolutely in line with the ones now discussed in order to reach interoperability at European level.

Finally, Spain has resolved very well the electronic identification of legal persons and enterprises through the emission of electronic certificates of legal persons / of representatives of entities with or without legal entity.

- As already mentioned, full development of Law 11/2007, which foresees electronic access to all public services, has been planned from two different perspectives, with common objectives:

Strategic Plan

The strategy to be carried out has as objective the adjustment of all public services and procedures to Law 11/2007 in the framework of the General State administration, including all its depending or linked organisms. This plan is focused in four strategies:

- Services based on the citizens
- Adjustment of procedures to Law 11/2007
- Infrastructures and common services

• Horizontal actions

All transactions and administrative services of the State Administrations, compiled in a public catalogue, will be available on-line before the 31 December 2009, at its highest level, according to a schedule that will be permanently updated.


Performance Plan628

According to the Strategic Plan, the Implementation Plan is based on three lines:

1. Public services for citizens, designed according to their needs, and adapted to their demands, guaranteeing equal access and non discrimination.

2. Adjustment and simplification of administrative procedures, according to Law 11/2007, and reducing the administrative burdens.

3. Availability of infrastructures and common services that will enable the development of new services and the interoperability of the existing ones, taking advantage of the cooperative work in similar implementation areas and respecting the ancillary principle, so that technologic solutions be at the service of management processes, obtaining the maximum profitability from investments in technology.

These lines complement each other with horizontal actions related to interoperability and security, training of public employees, management and follow up of the Plan, reuse of applications among Administrations, as well as drafting of reports on the development of eGovernment in Spain.

Altogether, their objective seeks to guarantee the benefit for citizens, integrating the performances carried out individually by each Ministry with other performances developed in a collective manner.

628 Document explaining the Performance Plan available at:
32 Sweden

32.1 General framework for electronic documents in eGovernment applications

32.1.1 Electronic documents in eGovernment applications

There is no Swedish legislation regulating a generic framework for electronic documents in eGovernment applications. Instead of being regulated in a specific or general law the numerous eGovernment applications offered to the public have been implemented by the different public administrations via their own web services. In some cases amendments in the legislation applicable to the service were necessary in order to allow the use of electronic documents or rather electronic identification, but specific requirements were usually adopted on the local level.

The Swedish approach has focused more on the exchange of information between public administrations on one hand and easier access to information for the citizens through the use of electronic ID cards on the other hand. The use of electronic documents as such has not been an issue for discussion.

In many cases the existing legal framework was interpreted in a way that allowed the use of electronic documents629, and in other cases the question mainly focused on securing the identity of the sender rather than regulating the use of electronic means as such. One of the few exceptions that dealt partly with electronic documents was the governmental report introducing a bill allowing auditors’ reports to be submitted in electronic format according to Swedish Companies Act (Aktiebolagslag (2005:551)).630

Therefore, the only general framework with regards to electronic communication concerns the electronic IDs (e-legitimation) that are being issued by private entities, mainly banks.631 Though there is no common legal framework for these eIDs - except some general rules in the Act on Qualified Electronic Signatures (Lag (2000:832) om kvalificerade elektroniska signaturer)632 - most of the eGovernment applications require the use of such eIDs.

631 See (in Swedish) http://www.e-legitimation.se/
632 The Act is available in English at http://www.pts.se/Archive/Documents/SE/Qualified%20Electronic%20Signatures%20Act%20_SFS%202000_832_En glish%20translation.pdf
In the beginning of 2008 Sweden adopted an Action Plan for eGovernment (handlingsplan för e-
förvaltning) aiming at more coordinated and strategic eGovernment measures within the Government
offices of Sweden. The plan includes four steps in order to achieve this goal. The first being a
harmonisation of rules that allow cooperation as well as an effective processing of information
increasing the accessibility and usability of the information while taking into consideration aspects of
integrity and security. The second step would then include an effective and stable infrastructure for
electronic communication. This standardisation of structures regarding terminology and information,
user interfaces and electronic communication should be done in accordance with the needs of the
public administrations as well as in coordination with international norms. Step three would then
consist of harmonising and automating the administrative support that the authorities share. In the
final step the contact with the citizens and companies should be facilitated and all public services and
information should be available both to citizens and companies.

The importance of electronic exchange of information between public administrations was already
stressed in a governmental report in 2007\textsuperscript{633}. The report focused, however, on the exchange
of information and not on the need for electronic documents as such.

Attempts of standardisation concern mainly the exchange of information, and there are about 915
strategic projects among 69 public authorities at the moment, the xbrl taxonomy\textsuperscript{634} (standard
messages) for annual revenues and similar economic information being the most significant one.\textsuperscript{635}

32.1.2 Electronic documents for the purposes of the implementation of the Services
Directive

A recently published governmental report analysed the necessary legislative and administrative
measures with regards to the Swedish implementation of the Services Directive\textsuperscript{636} and suggested the
issuing of a horizontal law containing some of the necessary amendments. In general, Swedish
legislation already fulfils most of the requirements stipulated in the Services Directive. Only a few
legislative amendments are necessary in this respect. In addition, however, the processes at the
public administrative level have to be amended and brought in line with the rules of the Directive. It is
also important to ensure that certain service providers present specific information when offering a
service. Therefore the report suggests a horizontal Act – the Act on Services on the Inner Market
(lagen om tjänster på den inre marknaden) – to come into effect by the end of 2009.

In order to facilitate the application procedures for service providers, the governmental report suggests
that the aforementioned Act should stipulate the creation of a Point of Single Contact. The

\textsuperscript{633} Increased electronic information exchange between public authorities - Utökat elektroniskt
informationsutbyte mellan myndigheter, SOU 2007:45, in Swedish at
http://www.regeringen.se/content/1/c6/08/37/51/287aea40.pdf

\textsuperscript{634} http://www.xbrl.se/14220.htm

\textsuperscript{635} Report by the Swedish (VERVA), 69 myndigheter redovisar 915 strategiska insatser för utveckling av e-förvaltningen,

\textsuperscript{636} Genomförande av tjänstedirektivet, Ds 2008:75, 24 oktober 2008, Utrikesdepartementet
Government or the authority appointed by the Government should regulate the details about this Point of Single Contact.

No specific mention was paid in the governmental report to the issuing of electronic documents with regards to the Services Directive. As mentioned earlier, the question has concerned, if at all, identification and not authentication of documents.

The implementation efforts have been focused in a first step into mapping which administrative procedures are relevant with regards to the Services Directive and which of these can or cannot be implemented via electronic means. Through an analysis of the relevant regulations and rules, the Government identified around 80 Swedish procedures to be covered.

In a second step the Swedish Administrative Development Agency (VERVA)\(^{637}\) was mandated to investigate the procedures even further. The analysis takes into consideration the amount and volume of the procedures, possible requirements for proof of identity and signature as well as access to register information. No specific attention is paid to the question of electronic documents as such. The report by VERVA should build the base for further development of electronic procedures and the interlinking with the Point of Single Contact.\(^{638}\)

The entity responsible for the creation of a single contact point is the National Board of Trade (\textit{Kommerskollegium})\(^{639}\) in cooperation with the Swedish Agency for Economic and Regional Growth (\textit{Nutek})\(^{640}\) and the Swedish Consumer Agency (\textit{Konsumentverket})\(^{641}\). At this point it is still unclear what technical solutions will be utilised. The National Board of Trade (\textit{Kommerskollegium}) is currently looking into different possibilities.
32.2 Specific document types

32.2.1 Extracts from commercial registers

In Sweden the commercial registers, such as the limited liability companies (aktiebolag) register, the trade register, the European companies register, the bank register containing information about the branches of foreign banks and the branch register, are held by the Companies Registration Office (Bolagsverket). The Office provides on-line access to this trade and industry register through a search function on their web site.

Information stored in the registers include, among others, registration number, name, address, board of directors, signatories and type of business activities. It is possible to receive selected information from the trade and industry register on paper or as files on CD.

Other information that can be ordered includes the certificate of registration, company’s annual reports (turnover, assets, liabilities, capital, etc) and extracts of accounts and copies of documents such as minutes of the annual general meeting or of board meetings.

The Swedish Companies Registration Office (Bolagsverket) also takes care of the European Business Register (EBR) that gives access to information on 20 million European companies in 18 European countries.

Information from the trade and industry register can also be accessed via sms. After sending an sms with the organisation number to the Companies Registration Office (Bolagsverket) one can receive the name of the company, the city, status (e.g. if company has ceased to exist) and the date when the last annual report had been submitted.

In order to access more information than the organisation number from the trade and industry register, one has to become a customer with the Swedish Companies Registration Office (Bolagsverket). This can be done by filling out the form available on the Offices website where after one receives a login and password sent to the home address. This service includes a fee based on the information that is being accessed.

As it seems, extracts from the Companies Register are not as such electronic documents fixed in their form, but rather different types of information than can be accessed online, either for free by anybody

642  http://www.bolagsverket.se/. A full list of the registers can be obtained in English at http://www.bolagsverket.se/in_english/in_our_registers/index.html
643  Information in Swedish at http://www.bolagsverket.se/sms/
644  https://snr4.bolagsverket.se/snrgrant/omTjansten.do
645  More information on prices at http://www.bolagsverket.se/in_english/products_services/
(concerning organisation number and name of company) or by subscription after being registered in
the system (all different types of information available). The question here does not concern any
electronic documents as such, but rather the identification of the user in some cases.

As Belgium, Sweden also participates in the BRITE Project\footnote{Business Register Interoperability Throughout Europe; see \url{http://www.briteproject.net/}}, which aims at interlinking European
business registers and therefore would facilitate the exchange of information even further.

### 32.2.2 Criminal records

In Sweden one can apply for an extract from the criminal records register \textit{(Registerutdrag)}. As
individuals can only access their own criminal record, a personal signature is required on the
application. No electronic means can be used in this process at the moment, other than the possibility
to apply for the extract by sending a scanned and signed version of the application via e-mail.\footnote{More information in Swedish at the website of the Swedish Police Service (\textit{Rikspolisstyrelse}), at \url{http://www.polisen.se/inter/nodeid=3606&pageversion=1.jsp}. An example of an application in English can be found in pdf format at \url{http://www.polisen.se/mediaarchive/4347/1541/2013/2016/Registerutdrag%20Engelsk%20RPS447_3b.pdf}}
Commonly the application has to be sent by letter or fax. The extract will then be delivered in a paper
form.

### 32.2.3 Extracts from professional registers

Commonly the professional registers are managed by private entities or organisations. Some registers
can be searched online, e.g. the register held by the Swedish Bar Association (\textit{Advokatsamfundet})
can be used when searching for a lawyer.\footnote{http://www.advokatsamfundet.se/templates/StartPage.aspx?id=12} Not being able to draw an exhaustive picture, it seems,
however, that traditional paper documents are still most commonly being issued.

The above-mentioned governmental report does not set up any plans on encouraging professional
organisations to utilise electronic documents to a greater extent. In the VERVA report, the Swedish
Bar Association as well as the Legal, Financial and Administrative Services Agency
(\textit{Kammarkollegiet})\footnote{Information in Swedish at \url{http://www.kammarkollegiet.se/tolktrans/tolktrans.html#}} concerning the authorisation of interpreters and translators were mentioned as
suitable for inclusion in the Point of Single Contact as soon as possible.
32.2.4 Certificates of insurance

There seems to be no general usage of certificates of insurance in electronic form in Sweden. Even in cases that allow electronic application processes, the certificates of insurance ("försäkringsintyg") can still be – and usually are - submitted via regular mail.

32.2.5 Proofs of qualifications

Sweden does not have a general framework regarding the issuing of proof of qualifications. These documents are usually issued by private organisations and commonly in paper form.

32.2.6 Statements from the service provider

As the technical solution for the Point of Single Contact has not been decided yet, it is difficult to foresee which technical requirements the service providers have to fulfil when it comes to statements. Probably the web service of the Point of Single Contact will include a technical solution in this regard. It is, however, not possible to predict any further technical details at the moment.

32.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

32.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

The above mentioned governmental report discusses the question that the Point of Single Contact (PSC) will entail several electronic communications with different public administrations regarding applications from service providers as well as decisions from public administrations. This role as an intermediary raises legal questions concerning the grey area between a service function by providing information vs. submission of electronic records vs. initiation of administrative cases.

Concerning communication between the competent public administration and the service provider, the report suggests that the authority has to communicate with the service provider mainly via the Point of Single Contact if the service provider has submitted the application via the Point of Single Contact.

The Governmental report also stresses the importance of identifying which controls of correct/incorrect submissions are possible within the service function of the public administration and therefore not constitute any exercise of public authority. This would also allow the inclusion of this type of function in the system of the PSC.
The above-mentioned report by the Swedish Administrative Development Agency (VERVA), published in June 2008, deals with the implementation of the Services Directive. As shortly mentioned, VERVA investigated the readiness of the numerous administrative procedures that are relevant for the implementation of Article 8 of the Services Directive. The results are based on a survey on 76 different types of proceedings among several authorities, both national as well as regional and local. The survey included four types of criteria that had to be answered, namely number of applicants from EU/EES member states; identification and signature; document and register information; and additional assessment of suitability.

Out of 76 procedures (46 on a national, 14 on regional and 16 on local level) several were deemed to be able to included in the contact point almost immediately as they fulfilled several of the criteria of the analysis and are therefore able to be transformed into electronic procedures. In addition, an important factor was the amount of applications from EU/EES member states. The Swedish Companies Registration Office (Bolagsverket) with its registration for new companies and foreign branches as well as the Lawyer’s Association (Advokatsamfundet) regarding EU lawyers and the Swedish Legal, Financial and Administrative Services Agency (Kammarkollegiet) regarding the registration of translators are in the first group that can be integrated in the PSC rather soon.

The Companies Registration Office (Bolagsverket) fulfils almost all criteria and also shows a high number of EU/EES applications. Regarding the Lawyer’s Association (Advokatsamfundet) the focus should maybe be put more on increased information rather than an automated application procedure. With regards to the Swedish Legal, Financial and Administrative Services Agency (Kammarkollegiet) the general amount of applications is low but easy to implement with electronic measures.

The report found that most procedures require the attachment of documents (64 out of 83) and even more the signature of the applicant (72). At the moment more than 75 % of the application are submitted via regular mail and have to be signed. Most procedures seem to be suitable for automation.

The report listed all investigated procedures and recommended in which cases the use of electronic measures is feasible already now, in the near future or later. The development of the platform as such has, however, not been decided yet, but is ongoing. As it seems, existing technical solutions, such as the one being used by the Swedish Companies Registration Office (Bolagsverket) allowing the registration of new companies, as well as the Entrepreneur’s Guide by the Swedish Agency for Economic and Regional Growth (Nutek) will be extended and further developed.

---


651 [http://www.bolagsverket.se/](http://www.bolagsverket.se/)

652 [http://www.nutek.se/sb/d/390](http://www.nutek.se/sb/d/390)
32.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

According to the Governmental Report on the implementation of the Services Directive the main channel of communication to the Point of Single Contact will be a website (service portal). The functions of the PSC should be made available as soon as possible in Swedish as well as in English. The Point of Single Contact should even include a service function (help-desk) that allows individuals to communicate with the PSC via telefax or electronic mail (in accordance with Section 5 of the Administrative Act (Förvaltningslagen (1986:223))).

The creation of the Point of Single Contact falls within the competence of the National Board of Trade (Kommerskollegium)\(^{653}\), which is responsible for questions on the inner market and also concerns information that already today is provided electronically by the Swedish Agency for Economic and Regional Growth (Nutek)\(^{654}\) in relation to the Entrepreneur’s Guide\(^{655}\) as well as information provided by the Swedish Consumer Agency (Konsumentverket)\(^{656}\) with regards to Consumer Europe.

According to the Government the National Board of Trade (Kommerskollegium) should have the main responsibility. It is, however, important that the Swedish Agency for Economic and Regional Growth (Nutek) as well as the Swedish Consumer Agency (Konsumentverket) are involved as their existing electronic service functions can be utilised when creating a Swedish PSC. A strategy like this one is also in line with the eGovernment Action Plan.

As it seems at the moment, the Entrepreneur’s Guide\(^{657}\) offered by the Swedish Agency for Economic and Regional Growth (Nutek)\(^{658}\) will be further developed to become the Point of Single Contact in Sweden. It is, however, unclear at this point what specific technical solutions will be utilised for the PSC.

\(^{653}\) http://www.kommers.se/
\(^{654}\) http://nutek.se/sb/d/113
\(^{655}\) http://www.nutek.se/sb/d/390
\(^{656}\) http://www.konsumentverket.se/
\(^{657}\) http://www.nutek.se/sb/d/390
\(^{658}\) http://nutek.se/sb/d/113
32.4 Assessment – Plans, progress and proposals for further harmonisation

32.4.1 Current plans and progress in the implementation of the Services Directive

The above-mentioned governmental report suggesting the introduction of a new Act on Services on the Inner Market (lagen om tjänster på den inre marknaden) is currently being reviewed by public administrations and other stakeholders. After comments from the different interest groups the government will submit a bill to the Swedish parliament.

At the same time the National Board of Trade (Kommerskollegium) in cooperation with the Agency for Economic and Regional Growth (Nutek) and the Consumer Agency (Konsumentverket) is developing the Point of Single Contact. This process will take place during 2009.

According to the governmental report the implementation of the Services Directive presupposes cross border solutions for electronic IDs and electronic signatures. Sweden can start with specific measures to initiate the introduction of electronic procedures. These measures include analysis and investigation of existing administrative procedures. Electronic identification and electronic signatures are also one of the main questions in the eGovernment Action Plan in Sweden.

32.4.2 Suggestions for further European support initiatives

As the main focus regards electronic identification and electronic signatures, the standardisation or cooperation concerning cross border solutions for eIDs seems to be one of the main questions. The two Swedish administrative procedures that support electronic identification require the use of the Swedish eID solution, which are at the moment difficult to obtain for a non-Swedish resident.

In addition, common standards for administrative procedures could be utilised, in accordance with Article 40.2 of the Services Directive.
33 United Kingdom

33.1 General framework for electronic documents in eGovernment applications

33.1.1 Electronic documents in eGovernment applications

No single framework exists regulating the nature of electronic documents which may be used within
the public sector. The Electronic Communications Act 2000, which sought to implement the European
Directive on Electronic Signatures, provides in section 7 definitions of the concept of electronic
signatures and by section 8 confers power upon the government to modify existing legislative
requirements which would inhibit the use of electronic communications by, for example, requiring the
use of traditional paper based signatures. Relatively little use has been made of this regulatory power,
something which is perhaps explained by the fact that rather few restrictions were in force prior to the
enactment of the legislation. The Companies Act 1985 (Electronic Communications) Order 2003 is
perhaps the most relevant piece of legislation and provides for the submission of company records
and accounts to be made in electronic rather than the previously required paper format.

In addition to few barriers preventing the use of electronic communications to and from Government,
incentives are sometimes offered to individuals and to undertakings to transact electronically with
Government agencies. These may, for example, take the form of extended deadlines for submission
of tax returns or a reduction in the fees payable to reflect the economies secured through the use of
electronic communications. Although some transactions may be conducted entirely electronically,
others, such as the issuance of vehicle taxation documents result in the issuance of a paper licence
document. Again, in cases such as this, as an alternative to the customer supplying physical or
electronic evidence such as their possession of vehicle insurance or a permit certifying that the vehicle
is in a satisfactory mechanical condition (MOT certificate), data will be exchanged either between
government departments or with trusted private sector agencies such as the Motor Insurers Bureau
which maintains a database of all car insurance policies. A number of other data exchange
agreements are also in force allowing, for example, photographs supplied in connection with driving
licence applications to be accessed also in connection with a subsequent passport application.
Following the publication of the Varney Report, ‘Service Transformation: A better service for citizens
and business in 2006 , a better deal for the taxpayer’ an initiative, generally referred to as ‘Tell us
once’ has been launched which seeks to minimise the need for citizens or businesses to provide the
same piece of information several times to different government departments.

In respect of electronic communications between Government departments and agencies, use is
made of the Government Secure Intranet (GSI). With infrastructure provided by Energis and data
centres and applications supplied by Fujitsu this was re-launched in 2004 linking over 140 local and
central government departments with over 280,000 users on a:

United Kingdom secure IP managed network, and (a) exchange and share Restricted (and
Confidential) information with other GSi community customers and other networks such as the
CJX, MoD, NHS and EU networks and (b) more safely access the public Internet. Standard
GSi services include wide area connections to customer sites, directory, mail relay, firewalls and anti-virus scanning. Other GSi services include anti-spam and anti-image scanning, application development and hosting, closed user groups, remote access for home or mobile workers and VOIP. Appropriately sponsored private sector companies may order GSi GSE services.

In conclusion, electronic documents are not normally either issued to or required from end users. More critical is the exchange of information in electronic form either between government and end users or within Government itself. In the latter context it is relevant to note the recent publication of the Data Sharing Review although the thrust of this is on the data protection implications of the sharing of personal data rather than the exchange of business related data. As indicated above, only a few legal requirements relating to the production of documents in specified paper format existed and the introduction of new requirements for electronic documents would in many respects mark a retrograde step.

33.1.2 Electronic documents for the purposes of the implementation of the Services Directive

Traditionally, the United Kingdom has imposed relatively few controls over those wishing to provide services. Some of the most highly regulated sectors, for example those concerned with health services, are excluded from the Directive. In the case of other professions, responsibility for entry and the maintenance of standards is delegated by law to nominated professional bodies. In perhaps the majority of cases, what will be involved is accreditation of non-UK qualifications and in most cases this process will be subject to the requirements of Directive 2005/36 which will take precedence over the Services Directive. Even in these cases, however, control operates largely in respect of the use of certain forms of nomenclature and in respect of access to certain facilities. Anyone can, for example, establish a business providing legal advice but only a person accredited by the Law Society may lawfully use the designation ‘solicitor’. Subject to some exceptions, it is generally the case that only accredited solicitors or barristers (in Scotland, Advocates) may appear in court as representatives of an individual or undertaking. Where licences or permits are required it is more common for these to be issued by local government authorities (of which there are around 450 in the United Kingdom) than by central government departments.

In addition to situations where permits are required prior to commencing business activities, there are a number of situations in which there is a requirement to notify an authority of the fact that an activity is about to commence in order to facilitate the possibility of a physical inspection. An example might concern the use of premises to supply cooked food. Although (with the possible exception of planning permission for use of premises for such a purpose) prior consent is not required, legal requirements relating to environmental protection and hygiene will apply.

In a policy document published in 2005, the ‘Transformational Government Strategy’ 660, the United Kingdom’s policies for modernising government services were laid down. Traditional structures, it was stated:

659 http://www.ogc.gov.uk/contractsdatabase/list_all_contracts_375.asp
are still paper-based and staff-intensive. The underlying assumption is that customers will fill in forms and that staff will process them by routine rather than by risk-managed exception. Telephone access, customer access over the web and other improvements have sometimes been grafted onto this base. This locks in high costs and difficulty in meeting changing customer or policy requirements. Choice is costly and slow to implement.

Historically government services depended almost entirely on form-filling and face to face meetings. Over the next decade, the principal preferred channels for the delivery of information and transactional services will be the telephone, internet and mobile channels – as well as the increasingly important channels within the digital home. Using customer insight, government will drive take-up of the best new digital channels and exploit mobile technologies; and it will innovate its services to take swift advantage of new technologies as they emerge.

One area highlighted for improvement concerned the number of government web sites. In 2005, there were over 2500 such web sites with each department having its own web presence. The quality of these sites was variable and had been the subject of criticism by the National Audit Office, which monitors public expenditure in terms, inter alia, of its value for money. A significant process of rationalization saw a number of sites closed and the remainder moved under the auspices of two web portals, Direct.gov⁶⁶¹ concerned primarily with the provision of information and advice to individuals and Businesslink.gov ⁶⁶² which, as the name suggests, is aimed at the business community and is the focus of most attention in the context of the United Kingdom’s implementation of the Services Directive, in particular in connection with the establishment of points of single contact. In its most recent review of Government services offered over the Internet, the National Audit Office published in July 2007⁶⁶³, signs of progress were identified:

There are indications that government web provision became more comparable with the best private sector websites in the period around 2003-04, and the vast majority of government sites have quite similar and effective levels of functionality and design. In our survey they are rated reasonably well.

In addition to the two web portals or in the Audit Office's terminology 'supersites’ the Government Gateway⁶⁶⁴ provides a means for individuals and businesses to register to communicate with government agencies. Registration is largely designed to provide a vehicle allow the identity of the individual or business to be verified. Once this has been done, use of the Gateway will facilitate access to services such as, for example, payment of personal or business taxes. Considerable emphasis is placed on the levels of security associated with the Gateway site; all information that is transmitted through a 128-bit Secure Socket Layer connection (SSL). The site also supports the use of digital certificates. In general, however, relatively little use is made of digital certificates in the United Kingdom. In many respects, the jurisdiction has tended to take a relatively lenient approach towards issues of identity management. Even where traditional forms of signatures have been required it has

⁶⁶¹ http://www.direct.gov.uk/
⁶⁶² http://www.businesslink.gov.uk/
⁶⁶⁴ http://www.gateway.gov.uk/
always been accepted that the use of mechanical forms of writing or even rubber stamps will suffice to comply with legal requirements.

33.2 Specific document types

33.2.1 Extracts from commercial registers

A wide range of business structures are available to those wishing to engage in business or professional activities within the United Kingdom. The Businesslink.gov web site provides information about the range of structures available\(^ {665} \) and interactive guidance as to the optimal form for any particular user. The main forms available are:

- Self-employment
- Sole trader
- Partnership
- Limited liability partnership (LLP)
- Public or private Limited liability companies
- Franchises

Although any economically active entity will be required to make appropriate contact with the tax authorities, it is only in the case of entities whose owners utilise vehicles such as a limited liability company which restrict or exclude their own personal liability for debts incurred by an undertaking that formal requirements tend to be applied in respect of public notification of establishment and financial performance.

All limited liability company require to file documents of establishment at Companies House, an Executive Agency of the Department for Business, Enterprise and Regulatory Reform (BERR). There are more than 2 million limited companies registered in Great Britain, and more than 300,000 new companies are incorporated each year.\(^ {666} \)

Executive agencies are organisations which operate under the ambit of a government department and which perform functions laid down under some form of statutory authority but which enjoy a degree of managerial and financial autonomy in respect of the performance of the tasks imposed on them under legislation. In the case of Companies House, the legal basis for its activities is to be found in a range of Companies Acts, principally the Companies Act 1995.

\(^ {665} \) [http://www.businesslink.gov.uk/bdotg/action/layer?r.l1=1073858805&topicid=1073865730&r.lc=en&r.l2=1073859131&r.s=tl](http://www.businesslink.gov.uk/bdotg/action/layer?r.l1=1073858805&topicid=1073865730&r.lc=en&r.l2=1073859131&r.s=tl)

\(^ {666} \) [http://www.companieshouse.gov.uk/about/functionsHistory.shtml](http://www.companieshouse.gov.uk/about/functionsHistory.shtml)
Key information relating to the structure of companies and the identity of directors requires to be filed (electronically if so desired) with Companies House at the time the company is formed and accounts are required to be submitted, again potentially electronically, on an annual basis. The information may be physically inspected free of charge by any person and electronic copies of basic information are available free of charge with more extensive documentation available upon payment of fees.

33.2.2 Criminal records

Access to criminal records is an important element of many licencing schemes especially in areas where the service provider might be in a position to expose members of the public to significant personal or financial danger. It is a common requirement for applicants to be asked to indicate details of any criminal convictions and a failure accurately so to do will normally render any agreements or permissions voidable.

The Rehabilitation of Offenders Act provides rules relating to the length of time for which convictions require to be disclosed. Depending upon the seriousness of offences, an individual may, after the passage of a number of years, generally answer in the negative in response to a question whether offences have been committed. Since the enactment of the Data Protection Act in 1984 (now in the form of the Act of 1998) it has been open to individuals to seek access to details of their criminal convictions. The 1998 Act contains provisions to make unlawful the demand by a third party, that access be sought on their behalf (enforced subject access). These provisions have never been brought into fore but following a number of high profile cases of individuals with previous convictions (or significant grounds of suspicion) being able to conceal details of their background, the Criminal Records Bureau has been established to provide a mechanism has been established to enable employers and others considering engaging anyone to work in specified capacities to obtain either a standard or enhanced criminal record from the Criminal Records Bureau and to present this to the potential employer. Two paper forms of record are provided for. A standard disclosure will give details of criminal convictions together with any formal cautions which may have been issued regarding the individual’s conduct. Enhanced disclosure, which is restricted to the most sensitive areas of activity – typically involving contact with children or vulnerable persons – include details of any more speculative data which may be held concerning the individual. Whilst third parties do not have a direct right of access to criminal record data, it is permissible in these specified circumstances for them to require the individual to seek access and present the results to them.

33.2.3 Extracts from professional registers

A wide range of professional registers exists, often associated with trade associations. There in no legal barrier to these associations making details of their members and their qualifications available in electronic form although in many cases the key requirement will be for the provision of some form of accreditation, possibly in the form of an card identifying an individual and his or her status within the organisation, which might be shown to consumers at the point of service delivery. In other instances, it may be that a party may seek access to an on-line register of members of a profession or trade in order to obtain re-assurance that a person with whom he is contemplating doing business is in fact registered with the association. In this, as in many cases, the prime requirement will be to be able to access information in electronic form rather than to obtain an electronic document per se.
33.2.4 Certificates of insurance

As a general rule, certificates of insurance are not issued in an electronic form. While it would be legally possible to do so under the terms of the Electronic Communications Act, in practice there seems to be no demand for electronic certificates, and so far there are no applications or services that require them, either in the public or private sector. Thus, the only electronic certificates of insurance that are encountered in practice are unsigned scanned documents (typically in pdf or tiff formats), which are occasionally used in cases where originals are not required.

33.2.5 Proofs of qualifications

The same comments made above in relation to certificates of insurance apply also to proofs of qualifications. Generally, these are provided in paper format, for example as a degree certificate from a university or college or as a certificate of accreditation from a trade or professional association. There is no legal barrier to the acceptance of electronic copies of such documents and it is possible in the case of some universities, for students to access transcripts of their performance electronically and, if so desired or required, to send copies of these to third parties in the form of email attachments. There would also be no barrier to a party scanning a copy of a paper certificate and forwarding this by email.

33.2.6 Statements from the service provider

As described below, it is the intention that the Point of Single Contact will collect information from potential service providers and inform competent authorities that the information is available for collection by them. It would appear that it will be open to the provider to submit such information as is considered relevant. It does not appear that any specific provision is envisaged for the use of electronic signatures but this is generally not a matter of major significance and work is ongoing to identify those areas where current legislation requires the provision of a signature to determine whether this can be considered an essential requirement.
33.3 Delivering electronic documents to service providers in the context of the Point of Single Contact

33.3.1 The back-office – communication between the Point of Single Contact (PSC) and the competent public administrations or private organisations

As has been indicated above, the United Kingdom makes available a wide range of government information and services in electronic format through its Businesslink.gov.uk portal. In many important respects this portal currently provides much of the functionality which will be required from Points of Single Contact under the Directive and it appears to be the intention of the United Kingdom Government that the implementation of the Directive will take place through this web portal. It is however, recognised that work will be required in order to link local authority websites more fully into the Businesslink.gov site and also to incorporate access to private sector bodies which are responsible for issuing licences and permits in specific areas. Issues are complicated by the fact that in some areas of activity, local authorities are given a choice whether or not to impose systems of licensing or registration. Hairdressers, for example, are required to register in some local authority areas but not in others. Businesslink.gov already has a function allowing requests for advice on legal requirements to be tailored according to the location(s) in which activity is contemplated.

In its response to the results of a consultation exercise on the implementation of the Directive, the comment was made that:

The Government’s approach will be to try and achieve the best mix of cost and benefits in the available timeframe. It is the view of the Government that trying to build what would be a highly complex ‘point of decision’ in time for the implementation deadline at the end of 2009 would expose the project to considerable and unacceptable risks. We agree with those competent authorities who argued that such a development would unnecessarily duplicate their functions and in our view this would also go beyond the immediate requirements of the Directive. The Government does however wish to put in place a PSC that can be enhanced over time, working with the appropriate stakeholders to ensure that developments deliver further benefits in proportion to their cost.

In justifying the decision to place reliance upon Businesslink, it was noted that:

The Government’s general policy towards using Business Link as the main interface between it and business has been set out in two reports: Transformational Government - Enabled by Technology (Cabinet Office, November 2005) and Service Transformation (Sir David Varney and HM Treasury, December 2005). The resulting Service Transformation Agreement included a commitment to “rationalising the plethora of government websites by closing down the majority and moving their citizen and business content to the Government’s two single access websites, Directgov and Businesslink.gov.uk thereby giving customers access to the information and services they need with greater speed and ease.”
Responsibility for many aspects of the law relating to the provision of services has been devolved from the United Kingdom Parliament to the devolved legislatures in Scotland and Wales. Few if any significant variations exist in respect of legal requirements and, with the agreement of the devolved administrations, the current proposal is that there should be a single United Kingdom Point of Single Contact.

One limitation of the current web portal is that it is essentially focused upon public services and public authorities and a degree of expansion will require to be provided in order to facilitate interaction with private organisations which, as for example in the case of CORGI, which is currently responsible for authorising any person who wishes to work in respect of the installation or servicing of gas fuelled equipment.\(^{667}\)

### 33.3.2 The front-office – communication between the Point of Single Contact (PSC) and the service provider

Although as noted above, consideration is being given to the inclusion of telephone and email support centres in conjunction with the Point of Single Contact, it is not envisaged that any significant physical presence will be involved.

In addition to the provision of information on the Web, support has been expressed by a number of parties for the provision of alternative forms of advice and assistance. In this respect it has been indicated that:

> On balance the Government believes it would be beneficial to provide both email and telephone support for PSC users as soon as practicable and will be investigating the options for such a service.

It is the intention of the Government that the point of Single contact should seek to capture the location of potential users by means of tracking their IP address. Whilst this cannot identify the nationality of a user, it can indicate the geographical location from which a communication originates. Such data may be used to provide at least initial basic information in a language appropriate to the IP location.

Currently, Businesslink provides a substantial number of links to other web sites relating to different aspects of authorisations that are required in conjunction with the provision of services. It is envisaged that this will require to be extended with discussions focusing on the extent of material that should be held within the Point of Single Contact. A collection of links to other sites would not, it is considered, meet the requirements of the Directive. Conversely, however,

> A fully encapsulated service (a Point of Decision) would see the PSC authorising the provision of a very wide range of services. This sort of “one-stop-shop” would enable users

---

\(^{667}\) From April 2009, the Capita Group will replace CORGI as administrators of the gas registration scheme.
of the PSC to access all necessary information and monitor the progress of authorisation requests until the PSC takes a decision on them. As a result service providers would only need to interact with the PSC, which would undertake the complete authorisation process. However, it would also require the PSC to take on responsibilities currently performed by the competent authorities, thereby either replacing them or providing duplicate procedures. This would make high demands on staff and resources for the PSC, greatly increasing the cost of delivery.

Such a system, though undoubtedly convenient for users, is likely to be extremely expensive to construct with some estimates suggesting set up costs of several hundred million pounds if all possible services are to be covered. The scale of this approach also increases the risks of the PSC not being implemented when due and of it providing incorrect information following any changes to requirements, should the organisation responsible for those requirements delay in adding the changes to the PSC.

As suggested in a scoping study produced for the United Kingdom Government it was suggested that the optimum solution would involve a compromise between the two approaches. As outlined in the Government’s consultation document, it was suggested that:

a range of provision which it described as “Pro-active Signposting” - more than just a list of links, but not incorporating all the functionality into one system. Under this approach, the PSC would help the user identify what licences and permissions were needed, the information required by the relevant CAs, and then to apply to the appropriate authorities. In effect, the PSC would facilitate a seamless electronic journey from information gathering through to completion of requests for authorisations. It may also be possible to monitor progress of applications with CAs through such a PSC. This would achieve some of the benefits of a “point of decision” without the duplication of responsibilities.

One area which is under consideration concerns the extent of the information which should be made available from the Point of Single Contact. Whilst the Directive requires only information about legal requirements specific to the particular activity it has been recognised that there would be value in providing information on more general legal requirements such as, for example, those relating to employment law. The distinction between matters which are covered by the Directive and those which fall outside its scope may not always be entirely predictable. Matters of health and safety law are excluded from the Directive but as was commented by the Health and Safety Executive:

668 http://www.hse.gov.uk/aboutus/europe/euronews/dossiers/services.htm

UK health and safety law also covers the safety of others who might be affected by a work activity, including the public. The ‘freedom to provide services’ provision, introduced by the European Parliament, ensures that Member States will be permitted to impose national requirements provided they are justified for reasons of public policy, public security (this includes public safety), public health or the protection of the environment. This means that HSE and local authority inspectors will continue to be able to enforce against service providers from Member States in the same way as against established service providers.

668 http://www.hse.gov.uk/aboutus/europe/euronews/dossiers/services.htm
Information on these points would clearly be at least useful and possibly vital to potential service providers.

In addition to information regarding legal requirements, it is also being considered how to deal with issues which, whilst not required by law, may impact significantly upon the viability of services. In some areas, whilst membership of trade associations may not be a legal requirement, public awareness of the association brand may be sufficiently high to render an application for membership a matter of practical reality. An example might be found in the field of travel agency services where, at least in respect of High Street operations, most customers are likely to look for an agency which has taken out membership of the Association of British Travel Agents (ABTA) and as a consequence will offer customers protection in the event that the agency should cease trading.

33.4 Assessment – Plans, progress and proposals for further harmonisation

33.4.1 Current plans and progress in the implementation of the Services Directive

As indicated above, the United Kingdom has an extensive electronic infrastructure in the form of Businesslink that can be utilised for the purposes of implementing the Services Directive. The major area of change will require to be the inclusion of private sector organisations within the scope of the service. In consultation it was suggested by the United Kingdom’s Chamber of Commerce that it would be better equipped than government to operate the Point of Single Contact. This view was rejected by Government but it was conceded that:

\[\text{We will consider, in particular, whether the inclusion of access to private sector business advisors would bring added value to potential PSC users and if so how and when to incorporate this. The Government does not rule out the possibility of the private sector being involved in the delivery of some support services within the PSC.}\]

The major outstanding areas in relation to the United Kingdom’s implementation of the Directive relate to the integration of local government and private sector regulatory activities within the scope of the Businesslink.gov website. Given the number of competent authorities (possibly approaching 600) there will almost certainly be significant discrepancies in the level of online expertise. At the initial stage, it is envisaged that the Point of Single Contact will collect information from service providers, notify competent authorities that the information has been presented and enable them to collect and process it. In the longer term, a push rather than a pull mechanism would be desirable but this will require more extensive linkages between IT systems.
33.4.2 Suggestions for further European support initiatives

Given the limited role played by signatures in the United Kingdom and the limited reliance expected to be placed on electronic documents as opposed to the electronic exchange of data, the role of electronic signatures is not currently a topic of major importance. In the areas where signatures are used, for example in the field of taxation, limited interest has been shown by users with the Treasury commenting:

The use of User ID and password has become the dominant method of providing secure access to online services across most of government and private sector services. It has been and remains the IR's central approach to access to secure online services. It also seems clear that agents' preference is for a User ID and password solution. And software vendors are also not seeing a great demand for DCs to be included in their products. Indeed the expense of doing so means that many vendors are pressing to exclude DCs from their products.

Although DCs are widely available, there has been a limited market take-up, and current take-up is now virtually static. There are only around 1300 customers who are registered with DCs for our online services and the number of actual users is probably a lot lower. There is very little demand to extend the number DCs that we currently accept.  

Standardisation issues are also seen as a barrier with the comment made that there are:

compatibility problems between operating systems and DCs, e.g. Microsoft XP users cannot use the Equifax DC, and these problems have both cost and support implications.

The view was put forward that the market for digital certificates was unlikely to grow in the coming years and that developments in biometric identification techniques might overtake electronic signatures. There does appear need for work both to develop more comprehensive standards for the current generation of signatures and to consider how biometric identifiers might be applied.

669 http://www hmrc gov uk/ebu/digital-certs htm