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

D3.1 Recommendations on improving the cross border exchangeability of electronic documents and interoperability of delivery systems for the purposes of the implementation of the Services Directive

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 (‘eDocuments Study’ or briefly ‘the Study’), focusing specifically on the availability and use 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 third and final report provides recommendations on how the Commission can assist the countries in improving the cross border exchangeability of electronic documents and interoperability of delivery systems; and how mechanisms can be provided to improve cross-border interoperability and collaboration with regard to e-documents and their delivery.
Document Change Log

<table>
<thead>
<tr>
<th>Issue</th>
<th>Issue Date</th>
<th>Description</th>
<th>Modified paragraphs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>9-Feb-09</td>
<td>First public draft</td>
<td>All sections</td>
</tr>
<tr>
<td>1.1</td>
<td>13-Feb-09</td>
<td>First public draft reviewed</td>
<td>All sections</td>
</tr>
<tr>
<td>1.2</td>
<td>25-Feb-09</td>
<td>Finalisation following internal discussions</td>
<td>All sections</td>
</tr>
</tbody>
</table>
Table of Contents

1 DOCUMENTS 6
1.1 APPLICABLE DOCUMENTS 6
1.2 REFERENCE DOCUMENTS 6

2 GLOSSARY 6
2.1 DEFINITIONS 6
2.2 ACRONYMS 6

3 INTRODUCTION 6
3.1 SCOPE AND OBJECTIVES OF THE PROJECT 6
3.2 STRUCTURE OF THE PROJECT 6
3.3 GOAL OF THIS DOCUMENT 6

4 SUMMARY OF THE ANALYSIS REPORT – KEY ISSUES AND THEIR IMPACT 6
4.1 MAIN FINDINGS OF THE ANALYSIS REPORT 6
  4.1.1 ON THE AVAILABILITY AND DELIVERY OF eDOCUMENTS 6
  4.1.2 ON THE ACCEPTANCE OF eDOCUMENTS BY PSCs 6
  4.1.3 RESULTING ISSUES 6
4.2 IMPACT OF THE CURRENT SITUATION AND ISSUES TO BE ADDRESSED 6
  4.2.1 THE NEED FOR ACTION: DO PSCs NEED eDOCUMENTS? 6
  4.2.2 RESPONSIBILITIES AND CHOICES 6

5 RECOMMENDATIONS FOR THE SHORTER TERM – IMPROVING INFRASTRUCTURE AND TRANSPARENCY, AND FACILITATING VALIDATION 6
5.1 INTRODUCTION AND OVERVIEW 6
5.2 FLEXIBILITY AND TRANSPARENCY - AVAILABILITY OF eDOCUMENTS 6
5.3 FACILITATING VALIDATION 6

6 STRATEGIC RECOMMENDATIONS FOR THE LONGER TERM – THE ROLE OF eDOCUMENTS AND INFORMATION EXCHANGE AT THE EUROPEAN LEVEL 6
6.1 eDOCUMENTS AND THEIR ROLE IN PUBLIC ADMINISTRATIONS IN GENERAL 6
6.2 REFINING THE eDOCUMENTS APPROACH AND CREATING ADDED VALUE 6
1 Documents

1.1 Applicable Documents

| AD1 | Framework Contract ENTR/05/58-SECURITY |

1.2 Reference Documents

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

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the definitions below apply to these notions and have also been used by the correspondents in their reports. Where applicable, definitions from the eSignatures Directive\(^1\) are observed.

- **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.
- **Authentic eDocument**: any eDocument that has been authenticated by its issuer using any means recognised under applicable national law, specifically through the use of electronic signatures.
- **Authentic database**: any data collection in which certain attributes of a clearly defined subset of entities are managed, and to which a particular legal or factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.
- **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.
- **IMI system**: the Internal Market Information system put into place to facilitate the validation of certain information between Member States, in particular in relation to professional qualifications\(^2\).
- **Electronic signature or eSignature**: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.
- **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.
2.2 Acronyms

A2A .............................................. Administration to Administration
A2B .............................................. Administration to Businesses
A2C .............................................. Administration to Citizens
CA ................................................ Certification Authority
CAdES ........................................ CMS Advanced Electronic Signature
CRL .............................................. Certificate Revocation Lists
CSP .............................................. Certificate Service Provider
eID ............................................. Electronic Identity
eIDM ............................................ Electronic Identity Management
IAM ............................................. Identity and Authentication Management
IDM ............................................. Identity Management
JPEG/JPG.................................... Joint Photographic Experts Group
OCSP ........................................... Online Certificate Status Protocol
ODF .............................................. OpenDocument Format
OTP .............................................. One-Time Password
PDF .............................................. Portable Document Format
PKCS.......................................... Public-Key Cryptography Standards
PKI.............................................. Public Key Infrastructure
PNG.............................................. Portable Network Graphics
PSC .............................................. Point of Single Contact
RTF .............................................. Rich Text Format
SA ................................................ Supervision Authority
SOAP .......................................... Simple Object Access Protocol
SCVP.......................................... Server-based Certificate Validation Protocol
SSCD................................. Secure Signature Creation Device
USB............................... Universal Serial Bus
TIFF.............................. Tagged Image File Format
TTP............................... Trusted Third Party
XAdES............................ XML Advanced Electronic Signature
XML.............................. eXtensible Markup Language
XML-DSIG....................... XML Digital Signature
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 electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive, in particular examining solutions used or planned to be used 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. 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 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. when required. This Study aims to examine if and how the Member States are currently using and/or planning to use such electronic documents, and which measures the Commission could take to support the Member States in this regard, 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 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 procedures as foreseen under article 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 approach 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

In the Analysis of Country Profiles, the current practices and plans in the surveyed countries regarding the acceptance and delivery of eDocuments for the purposes of the Services Directive were examined, along with an impact analysis looking at the consequences thereof on the functionality of the planned PSCs. As was noted in that report, a number of issues remain largely unaddressed, including the generally limited availability of eDocuments, the difficulties in validating eDocuments issued by services established in another Member State, and the substantial lack of any plans for the electronic delivery of eDocuments via the PSC. Not all of these issues are necessarily crucial for the operation of a PSC in compliance with the requirements of the Directive, as much depends on the implementation choices made by each Member State, and particularly on how far administrative simplification has been done. However, it is also clear that some of these issues will present real barriers within some Member States, and that many countries have expressed a desire for further guidance at the European level in addressing them.

In this third report of this Study, we will examine the measures that the European Commission could take to assist the countries in improving the cross border exchangeability of electronic documents and interoperability of delivery systems. Both short term and long term initiatives will be addressed; however, the emphasis of this report will be on short term actions, i.e. goals that could reasonably be achieved by the implementation deadline of the Services Directive at the end of 2009.

To accomplish this, this document consists of three parts:

- Chapter 4 below will provide a brief summary of the findings of the analysis report, as a background to which the recommendations of this report should be understood. This chapter will focus specifically on the impact of current choices and practices in the surveyed countries, and on the issues that need to be resolved to meet the requirements of the Services Directive;

- Chapter 5 will then provide shorter term pragmatic recommendations to address these issues. These recommendations will not focus on ideal solutions, but rather on efforts that could reasonably be undertaken to maximise the impact on the availability and cross border validation for eDocuments within the deadline imposed the Services Directive.

- Finally, chapter 6 will take a strategic perspective, examining the steps that would need to be taken to arrive at a more satisfactory solution in the longer term, extending beyond the implementation deadline of the Services Directive, and possibly beyond the scope of the Services Directive as a whole.
4 Summary of the Analysis Report – key issues and their impact

The previous report produced in the course of this Study, entitled the ‘Analysis and Impact Assessment Report’ (summarily referenced as the ‘Analysis Report’), examined if and how the surveyed countries were using or planning to use eDocuments in public sector applications, with a specific focus on their use (both acceptance and delivery) in the context of their PSCs.

4.1 Main findings of the Analysis Report

4.1.1 On the availability and delivery of eDocuments

On the availability and delivery of eDocuments, the Analysis Report noted that countries have thus far outlined their own approaches to the exchange of authentic information, but the role of eDocuments in these approaches is disputed. A large group of countries (37%) has no clear approach in place that is applied systematically throughout all echelons of public administration, but rather relies on ad hoc solutions that cater to the specific needs of each sector or application as they present themselves. Another group (17%) attempts to leverage their trusted networks for the exchange of authentic information, usually built around a commercial register connected to several other important databases, as a way of exchanging information without necessarily putting an electronic document in the hands of the citizen or business. Countries which have opted for this approach generally favour extending it to an international context, due to the increased efficiency and potentially greater security achieved by cutting out citizens and businesses as ‘middle men’.

Only 17% of countries have implemented an eDocument approach that relies to a significant extent on separate files signed with a PKI signature, which is the situation that could be considered as most closely analogous to traditional paper based delivery of documents. This approach was most frequently seen in relation to highly standardised documents managed and issued by public sector parties (such as extracts of commercial registers, where 37% of countries declared that electronic documents were available). In practice, these were virtually always PDF based, with other common formats more rarely being issued.

However, the observations above only apply to documents and eDocuments issued by public administrations. It is however clear that the scope of the Services Directive and of the PSCs can also include documents and eDocuments issued by private sector parties. This will notably be the case when a service provider needs to provide evidence of his membership to a professional body, copies of diplomas or proofs of adequate professional liability insurance. All of these documents are typically (though not necessarily) issued by the private sector.

When examining these document types, the availability of eDocuments was even lower. To a large extent this is the result of market forces: most countries noted that there were no real barriers left for the uptake of such documents by the private sector entities (most notably due to the implementation of
the eSignatures Directive\(^3\) and the eCommerce Directive\(^4\), but in practice very few if any of them delivered electronic documents. Most of the exceptions to this rule were unauthenticated documents (often PDF or TIFF scans) that were offered to requesting parties purely as a matter of convenience. Contrary to eDocuments issued by public sector parties however, the lack of availability of private sector issued eDocuments does not appear to be perceived as a real problem requiring further action.

Thus, the delivery of electronic documents in the form of authenticated files, either by public administrations or by private entities, is still rather rare. Key quoted reasons for this include a perception of limited business interest within businesses and with citizens; and the difficulty of establishing the authenticity of such documents, and specifically the competence of the signatory to sign these documents.

The overview above focuses on the delivery of eDocuments prior to the service provider’s use of a PSC (i.e. if and how a service provider can obtain eDocuments that could be submitted to a PSC). However, there is a second aspect that could also prove to be relevant, namely the delivery of eDocuments by the PSC to service providers who have used the PSC successfully (i.e. proofs of registration in business registers, etc.). However, this second issue does not appear to be clearly addressed in many countries at this stage, with the exception being the countries that have implemented a ‘secure mailbox’-approach for their PSCs, in which administrations will receive requests from service providers in their own secure mailboxes, and will be able to reply to the service provider’s mailbox. It should be noted that a lack of a clear approach in this respect may not be a problem under the Services Directive: article 8 requires that service providers 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 if this is needed. When the delivery of an eDocument is not necessary to start or exercise a service in a given country, it does not appear necessary for that country to implement a procedure to do so anyway.

4.1.2 On the acceptance of eDocuments by PSCs

Apart from the issue of delivery of electronic documents to service providers, there is also the question of acceptance of documents or information offered to the own PSC by service providers who are potentially established in any other Member State. Here, the main conclusion is that none of the surveyed countries appears to have a solution in place that allows them to verify the authenticity of original electronic documents. When a coherent approach to a PSC was reported, in all cases it relied on assurances from the service provider himself, possibly supported by (unauthenticated) copies of supporting documents. This assurance may result from the fact that a service provider has first authenticated himself in a secure environment and then uploaded copies of electronic documents on a specific portal, from the application of the service provider’s signature on the document (regardless of whether it was the original source of the document), or from the mere fact that the service provider states that the information is correct. Regardless, no country reports that it has a approach for validating authentic electronic documents from other sources than the service provider itself, apart from the possible appeal to the IMI system.

---


This observation is neither negative in itself nor illogical. Firstly, it is clear that one of the principal obligations of the Member States under the Services Directive is the consistent application of administrative simplification. There is an explicit rule in the Directive (article 5.3) which says that ‘a Member State may not require a document from another Member State to be produced in its original form, or as a certified copy or as a certified translation, except in the cases provided for by other Community instruments or where such a requirement is justified by an overriding reason relating to the public interest, including public order and security.’

In addition, it should be noted that many of the planned and/or partially implemented systems are quite sophisticated, despite their inability to validate authentic documentation from other sources than the service provider. However, one issue that is also largely unresolved (and related closely to the impossibility of validating foreign eDocuments from other sources than the service provider) is the lack of foreign eSignature support, i.e. the possibility of validating electronic signatures issued by CSPs in other countries than that of the PSC. Broadly speaking, none of the surveyed solutions has a clear approach for the support of eSignatures from other Member States in place yet, other than the reliance of currently ongoing European initiatives. While a number of the reports indicate that it is possible to integrate foreign signature solutions into the existing approach, there appears to be no clear approach in these countries to achieve this result by the end of 2009. In contrast, most countries appear to rely largely on the continuation and success of current European initiatives such as the establishment of a trusted list of CSPs to be supported (as currently examined in the CROBIES study), or for a smaller number of countries the establishment of a full validation platform.

Generally speaking, many of the countries expressed a desire for additional EU guidance, both in relation to eSignatures and eDocuments. With regard to eSignatures, the aforementioned trusted list initiative and standardisation work of the CROBIES project is frequently positively referenced, while a smaller number of countries prefer a validation platform instead. On the issue of eDocuments (and especially the question of whether more eDocuments should be made available, and if so in what form) there appears to be a significant measure of flexibility and good will within the surveyed countries. Generally speaking, the countries are open to additional guidance on the choice of document formats.
4.1.3 Resulting issues

In the Analysis Report, the main challenges to be overcome in the context of delivering and accepting eDocuments in the context of the Services Directive were briefly summarised as follows:

On the technical front, there is a significant degree of uncertainty regarding the support that the PSCs are expected to offer to foreign eDocuments, and on the choices that would need to be made with regard to each country’s own eDocuments to ensure that these meet the functional requirements. Specifically, it is unclear to the surveyed countries which technical choices they need to make to ensure that the eDocuments they deliver meet the requirements of other PSCs, both with regard to document formats and signature standards, and inversely what the characteristics of foreign eDocuments are that they might expect.

On the operational front, the surveyed countries are dealing with a number of pragmatic issues. The interaction with the relevant stakeholders in the private sector (insofar as necessary) is one of these elements: how can these stakeholders be integrated into the PSC, and how can it be ensured that information can be safely delivered from the service provider via the PSC to the stakeholder and back again? A second pragmatic issue that none the less causes some concern is the simple question of languages. Article 5.3 of the Services Directive states that certified translations may only be required in certain specific circumstances, but it is not yet clear how this rule will be applied in practice. This issue is even more pressing considering the use of Latin, Greek and Cyrillic alphabets in the impacted countries. No solution is in place yet with regard to these issues in most countries. In addition, there is the obvious issue that documents are often still only available in a paper format, and that electronic equivalents are largely missing, as noted above. How can Member States then deal with the conversion of paper documents into authentic electronic equivalents? Only a limited number of countries (most notably the Czech Republic, as will be commented further below) has foreseen a solution mechanism to this problem.

Finally, there is also a degree of uncertainty on the legal front. As was already noted above, it is currently very difficult to determine the legal value of (e)Documents (i.e. irrespective of whether they are presented in a paper or electronic form), both because of the difficulty of determining their origins and of determining their authenticity. Apart from invoking the assistance of the IMI system, no real solution to this issue is in place yet in most countries. It is unclear what kind of requirements countries can impose on documents and signatures issued in other countries. In a traditional paper based environment, the definition of documents and their formal requirements has always been a matter of national autonomy, in the sense that one Member State cannot dictate the form of documents issued in other Member States. It stands to reason that this same principle should be respected in an electronic environment (as indirectly confirmed by the equivalence rule of article 5.3 of the Services Directive). This can be particularly important in countries which intend to require the application of qualified signatures on certain document types in order for them to be considered legally valid under their jurisdiction. Finally, there are broader legal issues like the limitation of PSC response times and liability. Most countries have not yet provided an answer to these questions, although the reports frequently reference upcoming regulatory changes or reviews to rectify these issues.

However, it is not yet clear what the impact and relevance of these issues will be for the purposes of the Service Directive. This issue will be examined below.
4.2 Impact of the current situation and issues to be addressed

It is clear that any recommendations to be made must assist the Member States in achieving the goals of the Services Directive. Therefore, before going into specific recommendations to address some of the aforementioned issues, a question that needs to be examined first is the precise impact of the current situation, and to which extent further actions are needed under the provisions of the Services Directive. As we shall see below, the link between eDocuments and the Services Directive is not unambiguous and obvious.

4.2.1 The need for action: do PSCs need eDocuments?

A crucial question that needs to be addressed first is the necessity of eDocuments for the implementation of the Services Directive, and more specifically for the operation of a PSC. On this point, it should be noted that the provision of the Directive requiring the establishment of PSCs (article 8) is a part of the Directive’s chapter on administrative simplification. Indeed, the main goal of the PSC is to ensure that service providers can easily complete “all procedures and formalities relating to access to a service activity and to the exercise thereof” (article 8 of the Directive).

The use of eDocuments in completing these procedures and formalities is only addressed indirectly by the Directive, by noting in separate points that it must be possible to interact electronically and at a distance with the PSC (article 8.1, thereby acknowledging the role of electronic means of communication) and by introducing simplification and equivalence rules for the use of documents (article 5.3, thereby acknowledging the role of documentary evidence). Read jointly, it is clear that the Services Directive anticipates the important role that eDocuments may play in the operation of PSCs.

This does not imply however that eDocuments are legally speaking required in PSCs. To the contrary, article 5 of the Directive calls for the simplification of any procedures and formalities to the maximum possible extent, which includes the need to request authentic documentation or official translations. The elimination of supporting documents for certain types of services is certainly possible, for instance by replacing them by declarations of compliance from the service provider that it meets all relevant requirements imposed by the PSC.

Thus, the question of whether electronic documents are necessary is not determined by the Services Directive, but by the laws and policies of the Member States. The Services Directive merely requires the Member States to create a PSC that can be used to complete all procedures and formalities as noted above, and makes no statements on the necessity of eDocuments in this process. Similarly, with regard to authentic eDocuments issued by other parties than the service provider (i.e. eDocuments that have been authenticated through electronic signatures by such a third party), it is largely up to the Member State to determine for each type of service what the applicable requirements may be. The Directive only forbids Member States to ask for documents in their original form, as certified copies or as a certified translation, “save in the cases provided for in other Community instruments or where such a requirement is justified by an overriding reason relating to the public interest, including public order and security”.

Page: 17 of 34
Version:.................... 1.2
Issued on: ............... 25 February 2009
Ultimately, the use of eDocuments for the purposes of the Services Directive and more specifically for the operation of PSCs is determined by the national legal frameworks and policy choices. In this regard, it is important to note that several surveyed countries have noted that eDocuments will indeed be required for certain services in their PSCs, and that they are implementing the necessary infrastructure to support this necessity. As a result, the issues related to eDocument exchangeability become largely a matter of allocating responsibilities: whose task is it to ensure that eDocuments exist and that they can be used across borders, and what steps can be taken to facilitate this process?

4.2.2 Responsibilities and choices

The problem in relation to allocating responsibilities in resolving eDocument exchangeability can be most easily demonstrated by contrasting two fictitious Member States A and B that have taken positions at the extremes permitted by the Services Directive. Member State A has decided to take a very flexible approach: its PSC usually only requires confirmations of compliance from service providers, and if any supporting evidence in the form of eDocuments is needed, the submission of unauthenticated scans is deemed sufficient. Public administrations in Member State A do not issue eDocuments themselves, so these are not generally available. Member State B in contrast has emphasised security to a much greater extent: service providers need to submit electronically signed statements of compliance, often (when permitted by the Directive) supported by authentic eDocuments issued by the competent administrations. Furthermore, public administrations in Member State B typically issue authentic (electronically signed) eDocuments directly to service providers.

Problems will then inevitably arise when service providers established in Member States A and B try to access each other’s PSCs. The service provider established in Member State B will likely have little difficulties using the PSC in Member State A, as it has ample electronic means at its disposal, and the bar is generally not set too high. Inversely however, the service provider from Member State A may have a very difficult time in using the PSC from Member State B: the service provider simply does not have any authentic eDocuments to submit. In some cases, there may not even be authentic paper documents available (e.g. in cases where the PSC requires proof of enrolment in a professional register, while no professional register exists in Member State A).

To resolve this problem, it would again be possible to take two extreme positions. On the one hand, Member State A could argue that its PSC meets all requirements of the Directive (since it is accessible to all service providers), but that the PSC in Member State B does not, since it does not support the use by service providers in Member State A. Inversely, Member State B could argue that its PSC is perfectly operational, and that it cannot be held responsible for the lack of sufficiently advanced eDocument infrastructure in Member State A. These two extremes can be characterised respectively as a demand to simplify all PSCs to eliminate any usage barriers (which would however run afoul of legal requirements to submit authentic documents for some service types as permitted by the Services Directive) and as a demand to generalise the use of highly secure eDocuments in all echelons of public administrations (which would result in substantial costs and delays, and could be contrary to the Services Directive’s administrative simplification goals).

It is clear that the solution cannot be found in categorically choosing one option or the other, by shifting all burdens to harmonising all eDocument practices and standards or to simplifying PSCs to
the logical extremes. Rather, a common ground must be found that allows eDocuments to be usable in practice in cases where they are needed and add value to the process, and that can evolve if and when eDocument practices and PSC implementations in the Member States change.

In this respect the recommendations below take a two-pronged approach. The first set of recommendations, presented in chapter 5 below, emphasise elements that can be taken up in the reasonably short term and at a limited cost. They focus on progress that could conceivably be made within the implementation deadline imposed by the Services Directive, and that represents a realistic goal that the Member States can strive for within this term.

The second set of recommendations in chapter 6 takes a larger perspective, taking into account that eDocument practices and PSCs will not stop evolving after the implementation of the Services Directive, and also emphasising more strongly that the role of eDocuments should not be seen in a vacuum of the Services Directive, but rather that their role in eGovernment practices should be considered as a whole. While the short term recommendations try to focus on improving transparency and enabling eDocuments to function in practice, the longer term recommendations emphasise the need for coherence and added value within European electronic public administration as a whole.

For all of these recommendations, both short and long term, the central consideration is that the use of eDocuments is not a goal in itself. eDocuments are a means to achieve an objective, namely the exchange of sufficiently trustworthy information from one source to another. This is the goal that the recommendations ultimately serve to further.
5 Recommendations for the shorter term – improving infrastructure and transparency, and facilitating validation

5.1 Introduction and overview

As noted above, this first recommendations chapter will focus on improvements that could realistically be made within the implementation deadline imposed by the Services Directive. The goal of these recommendations is not to provide a complete and final framework for the handling of eDocuments in the context of PSCs, but rather to provide an approach that would allow PSCs to operate as required by the Services Directive.

To do so, we will focus on two specific themes:

- Firstly, ensuring the availability of the necessary infrastructure for the delivery of eDocuments, and improving transparency in relation to their availability. This theme focuses on the question of which documents should be made available in an electronic format and how this should be done.

- Secondly, the question of facilitating the validation of eDocuments, to ensure that eDocuments (if available) are actually of use to PSCs. In order for this to be the case, it should be possible for them to determine the authenticity of these documents in a relatively easy and accessible way.

Given that the implementation deadline of the Services Directive is relatively near, the present Study seeks to find a pragmatic low-complexity approach that presents significant benefits in the shorter term, and that allows the introduction of more advanced step-by-step improvements in the future without invalidating earlier efforts or investments.
5.2 Flexibility and transparency - Availability of eDocuments

As was noted in the overview above, the Services Directive does not inherently require the use of authentic eDocuments. Their availability and necessity is dictated by national regulations and policies, with some countries placing a stronger emphasis on the need for authentic eDocuments than others. Globally however, the Directive clearly recognises that Member States can be justified in requesting authentic documentation as a form of evidence in communications with the PSC, and as the country reports show, a number of PSC implementations will indeed require service providers to provide specific electronic documents to the PSC. However, several important observations can be made in this regard.

Firstly, authentic eDocuments issued to service providers are still relatively rare. This is true for public sector issued eDocuments, and even (much) more so for authentic eDocuments issued by private sector parties. In part, this can be explained by a lack of belief in the added business value for some of these documents, or simply a lack of demand from service providers themselves.

Part of this perception of limited value is the reality that authentic eDocuments are frequently difficult to validate by relying parties. Even when authentic eDocuments are used within a specific country, it is often difficult to determine their authenticity (by validating the electronic signature), and whether or not it was indeed issued by a party who is legally competent to do so (by determining the legal capacity of the signatory). This problem becomes even greater at the cross border level, where eSignature validation is currently almost infeasible and the exact origins of the document (the identity and competence of the issuing entity) are frequently very difficult to determine.

Of course, this difficulty in determining authenticity is certainly not unique to electronic environments. In a traditional paper based context it can be equally challenging to determine whether a document is authentic, and relatively superficial characteristics (such as letterhead, official looking stamps or signatures) are traditionally accepted as sufficient to consider a supposedly authentic document as acceptable. Thus, in a paper based environment there is a tradition of flexibility in accepting the authenticity of documents. While a conversion to an electronic environment offers possibilities to greatly enhance the reliability of verification processes, care should be taken that the migration from authentic paper documents to authentic eDocuments should not be taken as an excuse to introduce new restrictions and requirements with regard to authenticity that were not previously required in a paper environment. Such restrictions and requirements would run contrary to the spirit and the objectives of the Services Directive.

Indeed, the result of this lack of eDocuments, as was seen in the previous reports, is that existing PSC implementation plans do not include strategies to validate authentic eDocuments in any meaningful way. While many Member States invited further guidance to address this problem, and a small number of Member States had plans for the issuing of eDocuments by their own public administrations, none had put in place coherent and advanced strategies yet for the validation of authentic eDocuments issued by foreign entities. It is this issue that we aim to address.

As was noted above, in the course of this study we examined the availability of eDocuments issued by public administrations and by private sector organisations (such as professional bodies, insurance
agencies and educational institutions). The surveys showed that authentic eDocuments issued by private sector organisations were only very infrequently available, despite the fact that no substantial barriers to their issuance seemed to exist. In practice, the main factor in their unavailability seemed to be the perception of limited market demand for authentic eDocuments. More important for the purposes of this study was the fact that this unavailability of authentic eDocuments from private sector parties was virtually never identified as a problem that needed to be addressed before the PSCs would be able to operate. In practice, there seemed to be a large willingness to accept unauthenticated electronic copies of private sector issued eDocuments, and little desire to impose requirements on private organisation to issue authentic eDocuments. Given that further initiatives towards these documents would be rather complicated and do not appear to be seen as a priority, the recommendations of this study will focus exclusively on public sector issued eDocuments. It goes without saying however that some of the recommendations may have a spontaneous trickle-through effect on private sector issued authentic eDocuments in the longer term.

It would be unrealistic and impractical to propose a universal obligation on the Member States to make certain information (such as extracts from business registers or criminal records etc.) available in the form of authentic eDocuments, as in many countries the relevant information may simply not exist in the form of separate documents (even in a paper format) or even be kept systematically. Rather, our first recommendation is twofold:

- Firstly, public administrations that already issue eDocuments to citizens and businesses or that plan to start issuing such eDocuments should adhere to a common set of rules for eDocuments, irrespective of the sector in which the document is issued or of its contents. This first recommendation should result in a harmonization of eDocument issuing practices.

- Secondly, public administrations that manage authentic databases (electronic databases of reliable information) but that do not yet issue eDocuments based on these databases (such as the aforementioned examples of extracts from business registers or criminal records) should evaluate critically whether there would be an added value in doing so, based on the necessity in some cases for service providers to present this information to PSCs in other Member States. This second recommendation addresses the frequently recurring comment in some country reports that electronic resources were currently already available, but that extracts were not (yet) being issued electronically as there was no consensus on specific standards or formats.

Collectively, the goal of these first recommendations is not to make eDocuments mandatory to Member States that do not wish to work with them, but rather to ensure that countries have a series of pragmatic guidelines available to them that they can observe if and when they want to issue such eDocuments, to ensure that they can be used at the cross border level.

With regard to the common set of rules to be observed by such authentic eDocuments, these should initially be limited. The reason for this is the need to make progress by the implementation deadline, which is too near for an ideal solution to emerge already. Therefore, while semantic and linguistic coordination is advisable in the longer term to ensure that the contents of eDocuments in all Member States are comparable and understandable, this is not an objective that should be sought in the short term. Rather, the emphasis should be on ensuring that eDocuments are easily available, legible, and can be validated by the recipient to the maximum possible extent.

Therefore, only a limited set of requirements is presently imposed:
• As noted above, no semantic and linguistic harmonization is proposed in the short term, as this is not realistic given the implementation deadline;

• With regard to document format, it is recommended to adopt the Adobe PDF format, as this appears to have become the de facto standard for the vast majority of eDocuments surveyed in the Member States;

• With regard to signature format, it is recommended to move towards a consensus between the Member States on a signature format to be used universally for all authentic e-Documents issued by public administrations in the Member States, using the possibilities offered by article 8.3 of the Services Directive.

• Finally and perhaps most importantly, eDocuments should contain provide summary visual information on key characteristics of the eDocument to improve transparency and to facilitate their validation.

The last two elements will be discussed in greater detail in the section below (Section 5.3 – facilitating validation) to illustrate their envisaged impact.

This first set of recommendations is only helpful in cases where an eDocument is issued, but not in cases where no eDocument is available and a Member State has no intention of changing this situation. Such cases can never be fully excluded. For this reason, we recommend that PSCs provide easy communication mechanisms that the service provider can use when the requested documentary evidence is not available in its country of establishment. Thus, any request for documentary evidence should be accompanied by instructions on contacting the PSC when no equivalent documentation exists in the service provider’s country of establishment. This is part of the Services Directive’s obligation to accept as evidence “any document from another Member State which serves an equivalent purpose or from which it is clear that the requirement in question has been satisfied” (article 5.3), as this implies that the PSC communicates with the service provider to establish if an equivalent document exists. In cases of doubt, it goes without saying that the IMI system can also play a supporting role, most notably when it is unclear whether the claim that no equivalent document exists is truthful.

5.3 Facilitating validation

The second theme of the short term recommendations focuses on improving the possibility of validating authentic eDocuments on a cross border level, in particular by improving the communication of validation solutions to any relying party. Ultimately, the goal of this second theme is to ensure that countries have the possibility of validating authentic eDocuments from other countries without necessarily relying entirely on the IMI system. This should improve the autonomy of the countries and the efficiency of their PSCs.

To achieve this objective, we recommend first of all that certain information is visually stored in authentic eDocuments issued by public sector bodies (i.e. in a way that is immediately visible to relying parties when opening the document, rather than including it as non visible semantic information stored in the document). This information should be presented in a standardized and
easily recognizable form to improve its recognition in a cross border context, and should include as a minimum:

- The unambiguous identification of the entity responsible for the issuing of the eDocument, in accordance with nationally applicable rules, specifically its name in the nationally required language(s) and in English. This first data element should serve to make the issuing body more easily recognizable, which is an important factor in establishing trust in foreign documents. It should be noted that this proposal calls for the identification of the issuing entity, and not of the specific individual responsible for signing the eDocument (although this information may be optionally included as well; and in some cases the entity responsible for issuing the document is a specific individual). The main reason for this is that traditional paper documents in some cases only contain a stamp, but no information on the individual who applied the stamp. It does not seem logical or necessary to impose additional requirements on eDocuments than on paper documents. Furthermore, it should be kept in mind that the legal or factual authority linked to a public sector issued document emanates from the entity responsible for issuing it, and not from the individual acting on behalf of that entity.

- Unambiguous contact data of the entity responsible for the issuing of the eDocument, including address, phone number, fax number, website and e-mail address (if available). This information can be useful for purely pragmatic reasons, including when the relying party wishes to contact the entity directly for further validation, or to assist the IMI in its tasks if the relying party wishes to call upon the IMI's assistance.

- The name of the eDocument (e.g. ‘Extract of the Commercial Register’) in the nationally required language(s) and in English. Again, this is a purely practical recommendation that serves to alleviate some of the linguistic problems and the use of multiple alphabets in the European Union. The inclusion of a short descriptor can help in generating moderate confidence by providing a clearer initial indication of the nature and content of the e-Document.

- The exact date and time when the document was signed, for reasons of verification and legal certainty.

- The document number (Serial-No) which uniquely identifies a specific document issued for a specific service provider by a specific public administration (if available).

- Guidelines for the validation of the eDocument, at a minimum in English. This last element is central to the proposal, as it should provide the relying party with accessible instructions on the steps that he or she could take to determine the authenticity of the document. The complexity of this element depends entirely on the infrastructure that is available in the issuing entity’s country. In an ideal scenario, the validation instructions will point directly to a trusted validation portal where the document can be uploaded for automatic validation. In cases where no validation portal is available, validation instructions could refer to the IMI system.

It should be noted that this approach relying on providing visual validation clues in the eDocument itself is not a new approach. The Austrian use of a visual text box on eDocuments from the public sector is already quite well known, and provides an interesting example of this approach:
The Austrian approach is more advanced than the suggestion above, as it also contains technical information on the signature itself, to ensure that it can also be validated after being printed out.

Similarly, the e-Apostilles initiative relies on a standardized template of information to be included in electronic apostilles (documents created by public notaries in application of the Convention of The Hague of 5 October 1961 to attest to the authenticity of an official document in a cross border context). It goes without saying that the scope of apostilles is somewhat different than that of eDocuments, as apostilles are attached to original documents (in paper or electronic format) to attest to their authenticity, whereas the proposal above aims to replace paper originals by electronic equivalents.

None the less, the operational principles are broadly the same. Similar to the Austrian example, the template requires the public notary to provide clear information to identify himself and the document to which the apostille is appended.
While the standardized template above is relatively simple in appearance, the example presented below (issued in Colombia\(^5\)) demonstrates that the visual appeal of such documents can of course be improved to more closely resemble traditional paper based official documents, which can be important from a purely psychological perspective to inspire confidence (as in paper environments, where any objective indicators of reliability are also frequently lacking).

\(^5\) Currently, only Colombia and the US state of Kansas issue e-Apostilles, as noted on [http://www.e-app.info/documents/status_chart.pdf](http://www.e-app.info/documents/status_chart.pdf)
As noted above, apostilles are issued by notaries public and are always appended to an official document to attest to its authenticity, whereas an eDocument as we have described it would in principle be issued by the responsible public administration itself. However, this same approach could also be applied when relying on trusted third parties for the creation of authentic eDocuments. This option was also explored as a method of converting paper original documents into authentic eDocuments in the earlier ‘Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures’.

As noted in the Analysis Report, the Czech Republic has indeed implemented an authorized conversion procedure in its Act on Electronic Operations, to convert paper documentation into electronic documents and vice versa. Similar to the e-Apostilles initiative, this mechanism will rely on the intervention of notaries, regional authorities, registry offices, and some of the municipal offices and representative authorities to intervene by producing signed electronic copies of paper documentation.

---

It is clear that this approach is compatible with the proposal above, provided that these authentic (or perhaps more appropriately: certified) eDocuments contain sufficient information to allow their validation.

In that respect, it is interesting to note that both the Austrian system and the e-Apostilles programme have supplemented their approaches with validation portals (‘e-Registers’ under the terminology of the e-Apostilles programme) that can be used to validate their respective eDocuments. Thus, proofs of concept of this approach already exist.

While functional, it is clear that there are also drawbacks to relying fully on validation mechanisms which need to be duly considered. Apart from the need to introduce compliant eDocuments (which is admittedly a problem that would need to be addressed by any eDocuments approach) or to provide for acceptable conversion strategies relying on TTPs, the low complexity of this system means that it still involves personal intervention to validate eDocuments. To reduce this problem to some extent, it is also recommended to move towards a consensus between the Member States on a signature format to be used universally for all authentic eDocuments issued by public administrations in the Member States.

As long as there is no agreement between the Member States on signature formats used in the cross-border context, the automatic validation of authentic eDocuments in applications or the Points of Single Contact remains difficult. It is necessary to take action on this issue in the short term, as many Member States have indicated that they are reluctant to invest in eDocuments due to a lack of a common approach regarding electronic signatures between the Member States. Delaying a decision on the question of signature formats could therefore result in less eDocuments being issued by Member State administrations, an increased complexity for PSCs to accept such eDocuments, and thus ultimately additional expenses for the Member States. The current discussions and activities surrounding the proposal for an advanced electronic signature reference format in the framework of the Action Plan on e-Signatures and e-Identification 7 offer a framework to address and resolve these issues.

Greater advantages would be possible by taking an even more far reaching harmonization approach. By way of example, one might consider an alternative recommendation to deploy a system of ‘official signatures’ (as is currently being done in Austria), where each civil servant is issued a signature solution based on a standardized certificate that clearly indicates his or her official capacity, and which could then be used to sign eDocuments in accordance with the aforementioned harmonized signature standards to be established at the European level. Once this is done, a European trusted list could be established that details all official signatures in use in all of the Member States. Similar to the approach suggested by the CROBIES project, this would offer substantial benefits to the approach suggested above, as all Member States would then be able to implement more advanced and automated validation mechanisms into their PSCs. However, it is also clear that this approach would not be achievable within the deadlines of the Services Directive, due to the substantial additional difficulties that would need to be overcome in comparison with the scope of the CROBIES project, with key differences being the almost complete lack of official signatures in Europe today (with Austria being the only exception), and the lack of any supervision model over such signatures (which is one of

the basic building blocks in the CROBIES project). For this reason, the more pragmatic approach outlined above is suggested in the shorter term, even if it is more labor intensive in practice. However, it goes without saying that evolutions in the future may well lead to the establishment of a more advanced system relying on official signatures.

It is clear and acknowledged that the recommendations presented in this section do not create an ideal and conclusive framework for the use of authentic eDocuments. One remaining pragmatic question is how to trust validation mechanisms established outside the IMI system. Referring to the validation portals offered by Austria and the e-Apostille project, it is clear that these can only create trust in eDocuments provided that a relying party can actually determine the reliability of the validation portals themselves. If a relying party does not know if a website claiming to be a validation portal is trustworthy, any confirmation of authenticity provided by that website is of limited value.

However, a number of elements must be considered that mitigate this criticism. Firstly, it should be noted that the approach and reliability of the proposed approach is indeed not substantially better than what was previously possible in a paper context. For paper documents, relying parties from other countries who questioned their validity typically only had the choice of rejecting the paper document, or trying to obtain additional information from the entity that provided it or that claimed to have issued it. None of these options provided a significant additional assurance of authenticity. Even in its most basic form, the use of electronic signatures and validation mechanisms offers at least one additional benefit, which is the assurance that the document was not tampered with after its issuance. Thus, the current proposal inherently offers an (admittedly marginal) security benefit over traditional paper processes.

But secondly, and more importantly, it should not be overlooked that initially the IMI system can play a substantial role in creating trust in authentic eDocuments, by offering a universally trusted contact point for validation. The current proposal supports this function in two important ways:

- It requires certain essential information in relation to the authentic eDocument and its issuer to be included on the eDocument itself, thus facilitating the tasks of the IMI system itself;
- If a validation mechanism exists, then the current proposal provides an indication of what the IMI system will do to determine the authenticity of an authentic eDocument. This is important for a pragmatic reason: if a PSC questions whether a validation mechanism is trustworthy (which will initially be the case very frequently), it can submit the eDocument to the IMI system. If the IMI system then confirms that the validation mechanism was reliable, the PSC knows that it can use the validation mechanism itself in the future and rely on its output. This can prove to be quite beneficial, primarily because most Member States will see the majority of their PSC usage coming from neighboring countries. This means that familiarity with a limited number of validation mechanisms from a limited number of countries will already be adequate to process a significant number of PSC applications. After a limited number of confirmations from the IMI system, PSCs would thus be able to determine the authenticity of validation mechanisms themselves.

Finally, it would of course also be conceivable for Member States to publish references to reliable validation mechanisms on their own eGovernment websites, which would be a more direct way of creating this trust.
In this way, the weaknesses of the proposed approach can be managed in the shorter term. Obviously, in the longer term further refinements and additions are possible, as will be shown through the recommendations in Chapter 6 below. Meanwhile, the short term recommendations offer the possibility of making the validation and use of eDocuments in a cross border context feasible, while enabling a process in which the initial disadvantages can be gradually overcome without invalidating earlier choices and investments. It thus presents a step by step migration approach to a more effective exchange of trustworthy electronic information.
6 Strategic recommendations for the longer term – the role of eDocuments and information exchange at the European level

The short term recommendations in Chapter 5 above focused on improving the availability of eDocuments, increasing the transparency of their scope, and on providing a workable validation model. However, in the longer run, more security and greater ease of use should be possible. This second recommendations chapter will attempt to provide some guidelines to ensure that this happens in practice.

6.1 eDocuments and their role in public administrations in general

A key observation to be kept in mind is the comment that was already made above: eDocuments are not a goal as and of themselves, but merely a means of providing a sufficiently secure way of transporting information from one point to the other. In this respect, the delivery and acceptance of eDocuments represent an evolution of traditional paper based processes, rather than a revolution that aims to capture the full potential benefits of modern information technology. One could argue that it would be more advisable to take a longer term perspective, focusing on optimising the exchange of authentic information in eGovernment in general, rather than focusing on the narrower issue of eDocuments in the context of the Services Directive.

This observation was also made by a smaller number of countries in the course of this study, who noted that it would be more productive not to look at eDocuments as such, but rather to rely on interconnecting authentic databases into trusted networks for the direct exchange of authentic information. A frequently quoted reference of such an initiative is the BRITE Project⁸, which aims at interlinking existing business registers in order to facilitate the exchange of authentic information stored in these databases. Such solutions can be more effective and secure than the use of eDocuments, principally because they eliminate a risk factor in the communications process, namely the involvement of a citizen or business who acts as the recipient of an eDocument and transfers it from the issuer to the destination. Instead, the information is directly transferred from one authentic source to the party that requires it, reducing the risk of data corruption.

Such an approach could theoretically be expanded to a number of other fields in addition to business registers, including e.g. databases of regulated professions, which already exist in some of the countries. None the less, this is only feasible as a longer term objective to be strived for, due to the large number of issues to be overcome for most types of information, including most notably:

- the fact that authentic databases must exist in all participating countries, since otherwise no authentic information is available to be exchanged;
- these authentic databases must put the required infrastructure in place to be able to securely exchange information, based on common standards and protocols;

⁸ See http://www.briteproject.net/
the requirement for the information in the authentic databases to be standardised to a very large degree, since it is otherwise impossible to determine what the exchanged information means; this also means that the model is only applicable to types of information which are fairly uniform and standardised, which will often be the case for databases of official information managed by the public sector, but less so for types of information that might show larger variations;

the need to map access rights between all members of such a network, which requires at a minimum that local trusted contact points are established in each country, and that these contact points do not disseminate any information from the authentic network to third parties who are not allowed to obtain access to it;

in addition, in some countries authentic information might be stored by private sector partners, which could raise questions regarding the acceptability of this information in other countries that have no private sector involvement for comparable data, or at least regarding the desirability of exchanging information with these partners;

in relation to this, data protection issues must be duly considered to ensure that personal data is not processed contrary to applicable law;

finally, legal issues related to responsibility and liability for the accuracy and completeness of the information must be resolved.

It is clear that the establishment of trusted networks of authentic databases offers more promise and more potential advantages than an approach that relies purely on the use of authentic eDocuments, both for eGovernment in general and in the context of the Services Directive. However, the overview above also shows that it is substantially more complicated to establish such networks. While their creation and use in the longer term is certainly recommended, it is also advisable to examine the feasibility such networks on a case by case basis, and to take a gradual approach to deploying them. Thus, for the shorter (and even medium) term, their potential at the cross border level for the purposes of the Services Directive appears to be limited.

Notwithstanding this conclusion, it is possible to refine the approach outlined in the short term recommendations to a substantial degree in order to increase the utility of authentic eDocuments in general, and to improve their value as a part of the PSC’s operation. Possibilities and recommendations for doing so will be outlined below.
6.2 Refining the eDocuments approach and creating added value

As was noted above, the suggested short term approach of a limited harmonisation of eDocument practices has a number of advantages (mostly its limited cost and timescale in comparison to any alternatives), but also a number of disadvantages (mostly its suboptimal trust model, labour intensiveness and lack of semantic and linguistic clarity). However, many of these issues can be eliminated gradually by evolving to a more advanced infrastructure over a period of multiple years. For some document types, this will result in a gradual migration towards a trusted network model as described above; for others, eDocuments will remain a longer term solution as well.

Generally, the following steps are recommended to be taken in order to refine the proposed approach to eDocuments:

- As noted above, Member States should strive to ensure that validation mechanisms are available for any authentic eDocuments that their public administrations issue, to permit their validation without necessarily falling back on the IMI system for assistance. Ideally, this would already be the case immediately, but in all likelihood a transition period will be needed where validation platforms are not yet available in most countries. Member States should strive to offer only one single validation mechanism rather than a multitude of validation mechanisms, or at least they should ensure that one contact point is available where an overview of official validation mechanism can be found. This will address the problem of establishing trust in validation mechanism, which is much greater when there is no clear overview of trustworthy solutions.

- In a second phase, these validation mechanisms can be refined to further improve trust and to increase the efficiency of the system. Drawing upon the experiences of the CROBIES study, this could be achieved by establishing a system of ‘official signatures’ (electronic signatures used by public officials for the issuance of authentic eDocuments), in accordance with common signature standards and certificate profiles to be established at the European level. On the basis of this national infrastructure, a trusted list of official signature solutions could be created that would allow recipients of authentic eDocuments to determine the authenticity of the source of the eDocument (i.e. to determine if the eDocument was indeed issued by a competent administration based on the information in the certificate). This would resolve a trust question that was never duly addressed in a paper environment, thus creating greater benefits from the transition to electronic processes.

- In the following phases, the more complex semantic and linguistic issues can be addressed. For the most frequently used types of authentic eDocuments, semantic templates should be established that could be applied by all Member States, including a clear definition of vocabularies to be used for these documents. Once finalised, these should be used for the affected eDocument types, which will then be created in structured rather than unstructured formats. At this point, the language of an eDocument is no longer relevant, as it will be possible to convert any standardised eDocument into any supported language without affecting the meaning or legal validity of the eDocument.
In the final phase, it can be evaluated which eDocuments would no longer be necessary in the communication between public administrations or other trusted parties, by relying on trusted networks of authentic databases to directly exchange authentic information as described in the section above. As authentic eDocuments have already been fully standardised and made semantically interoperable at this point, the creation of such trusted networks will be largely a matter of assessing the political and legal feasibility of this evolution, in particular keeping into account data protection issues.

eDocuments are not static, nor a goal onto themselves. We believe that the approach above is sufficiently flexible to assess at each point which evolution is desirable, keeping into account the full technological, legal and policy context.