Common Solution Model
Draft Report on the completion of the reference model (D3.4)
Draft Report on the framework required (D3.5)
Draft Report on an appropriate governance model for the framework (D3.6)

Completion of the framework for Signature Validation Services

March 2010
This report / paper was prepared for the IDABC programme by:

Author: Hans Graux (time.lex), Olivier Delos and Sylvie Lacroix (SEALED)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°14

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://ec.europa.eu/idabc/

© European Union, 2010

Reproduction is authorised, except for commercial purposes, provided the source is acknowledged.
Executive summary

In earlier reports of the EFVS study, we have examined the feasibility of European scale electronic signature validation services, including the possibility of creating European level signature validation functionality based on a federated model of local (e.g. national) validation service providers. However, the consecutive reports showed that the establishment of such a functionality (and of signature validation services in general) was presently extremely challenging at the cross border level, as there was little consensus between the examined validation solutions on the types of services to be provided, and because there were still a substantial number of open issues, including with respect to certificate quality, signature quality, signature validation policies, long term validation, semantics, liability, relationship between the stakeholders (validation service providers, CAs, relying parties and signatories), etc. In practice, validation service providers need to address these questions themselves, with little guidance at the European or international level on which choices appear to be the most appropriate. This makes it very complex to establish a signature validation service capable of operating at the European level.

This report examines how these gaps can be filled in a way that would allow such validation service providers to operate at the European level within a consistent and comprehensive framework, covering the remaining legal, technical and trust challenges. The approach taken in this report is an open one, in the sense that the proposed steps are designed to be beneficial to eSignature interoperability as a whole, and not only to the operation of signature validation services. The different measures aim to progressively eliminate all barriers to the use of eSignatures at the European level, so that the usage of signature validation services will be the result of a choice to simplify matters for the relying party, rather than a matter of necessity.

In addition, the approach presented in this report is a progressive and stepwise one, which builds on the existing legal, technical and trust framework. The goal is to extend and reshape this framework, without invalidating any of the positive achievements of the current framework. In this way, the European eSignatures framework can be gradually recast into a comprehensive and fully consistent package, capable of addressing interoperability challenges for eGovernment services, as well as in any other contexts.
TABLE OF CONTENTS

EXECUTIVE SUMMARY 3

1 DOCUMENTS 5
1.1 APPLICABLE DOCUMENTS 5
1.2 REFERENCE DOCUMENTS 5
1.3 ACRONYMS 6

2 INTRODUCTION 8
2.1 THE EFVS STUDY 8
2.2 GOALS OF THE PRESENT REPORT – ADDRESSING IDENTIFIED PROBLEMS FOR eSIGNATURE VALIDATION THROUGH A COMPREHENSIVE FRAMEWORK 10

3 SUMMARY OF ESIGNATURE VALIDATION CHALLENGES 11
3.1 CURRENT eSIGNATURE CHALLENGES 11
  3.1.1 KEY SUCCESS FACTORS FOR eSIGNATURES 11
  3.1.2 STRENGTHS OF THE EUROPEAN eSIGNATURES FRAMEWORK 13
  3.1.3 WEAKNESSES OF THE EUROPEAN eSIGNATURES FRAMEWORK 14
3.2 SPECIFIC CHALLENGES FOR eSIGNATURE VALIDATION 17
  3.2.1 DESCRIBING AN IDEAL SIGNATURE VALIDATION SOLUTION 17
  3.2.2 DEFINING THE BUILDING BLOCKS, SERVICES AND STAKEHOLDERS 19
  3.2.3 CURRENT CHALLENGES FOR SIGNATURE VALIDATION SERVICE PROVIDERS 23
    3.2.3.1 Legal gaps 23
    3.2.3.2 Technical gaps 24
    3.2.3.3 Trust gaps 25

4 THE NEED FOR A BROADER PERSPECTIVE ON ELECTRONIC SIGNATURES, SIGNATURE VALIDATION AND OTHER CSP SERVICES. 27
4.1 INTRODUCTION 27
4.2 eSIGNATURES, eSIGNATURE VALIDATION AND OTHER TSP SERVICES 28
4.3 CONCEPTUAL MODEL FOR A RATIONALISED AND COMPREHENSIVE eSIGNATURE FRAMEWORK 30
  4.3.1 FROM A LEGAL PERSPECTIVE 30
  4.3.2 FROM A TECHNICAL PERSPECTIVE 32
  4.3.3 FROM A TRUST PERSPECTIVE 33
4.4 STEPWISE AND PRAGMATIC ROADMAP TOWARDS A SUCCESSFUL FRAMEWORK FOR INTEROPERABLE AND CROSS-BORDER eSIGNATURES 34
  4.4.1 LEGAL TRACK 34
  4.4.2 STANDARDISATION TRACK 36
  4.4.3 TRUSTWORTHINESS TRACK 37
  4.4.4 PROPOSED TIMELINE 38
1 Documents

1.1 Applicable Documents

<table>
<thead>
<tr>
<th>[AD1]</th>
<th>Framework Contract ENTR/05/58-SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>[AD2]</td>
<td>Project Management and Quality Plan (EFVS SC14 PMQP)</td>
</tr>
</tbody>
</table>

1.2 Reference Documents

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[RD2]</td>
<td>Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications</td>
</tr>
<tr>
<td>[RD3]</td>
<td>CROBIES study (Cross-Border Interoperability of eSignature), Siemens, SEALED and time.lex, staged publication: draft documents delivered in October 2009, last publication foreseen 1Q2010</td>
</tr>
<tr>
<td>[RD5]</td>
<td>Mandate M460, Standardisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to electronic signatures, 7 January 2010.</td>
</tr>
</tbody>
</table>
1.3 Acronyms

Au°A............................................. Authentication Authority (Authentication Services Provider)
CA............................................. Certification Authority¹
CRL ............................................. Certificate Revocation List
CSP ............................................. Certificate Service Provider¹
DSS ............................................. Digital Signature Services
DVCS ......................................... Data Validation and Certification Server
EFVS ............................................. European Federated Validation Service
IDABC ......................................... Interoperable Delivery of European Services to public Administrations, Businesses and Citizens
Id°A............................................. Identification Authority
LTAA ............................................. Long Term Archiving Authority
OCSP ............................................. Online Certificate Status Protocol
PKCS ............................................. Public-Key Cryptography Standards
PKI ............................................. Public Key Infrastructure
SCVP ............................................. Server-based Certificate Validation Protocol
SP ............................................... Signature Policy
SPA ............................................. Signature Policy Authority (Signature Policy Issuer)
TSP ............................................... Trust Service Provider
TTP ............................................... Trusted Third Party
TSA ............................................... Time Stamping Authority
TSL ............................................... Trust-service Status List
TST ............................................... Time Stamp Token
VA ............................................... Validation Authority

¹ It should be noted that in this report, the notion ‘Certification Service Provider’ or ‘CSP’ is used as defined in the Signatures Directive, namely as a “an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures”. The notion ‘Certification Authority’ or ‘CA’ is used as a subclass of CSPs, specifically as a CSP issuing signature certificates to the signatories. The latter notion is not defined by the Directive.
VSP........................................... Validation Service Provider
XAdES........................................ XML Advanced Electronic Signature
XKMS .......................................... Xml Key Management Specification
XML ............................................ eXtensible Markup Language
XML-DSIG ................................. XML Digital Signature
2 Introduction

2.1 The EFVS Study

The European Federated Validation Service (EFVS) Study aims to assess the feasibility of specific measures to ensure the availability of a European scale federated electronic signature validation functionality. The preceding reports analysed a set of existing signature validation solutions, along with the currently existing framework for signature validation, and examined the existing barriers that impeded the European scale validation of electronic signatures.

The analysis showed that validation solutions currently have two options for creating trust at a cross border level. The first option is to leverage the existing trust model that has been created by the eSignatures Directive, which created the concept of the qualified certificate and made this subject to national supervision. This means that qualified certificates can benefit from an inherent trust, caused by a common legal framework (the Directive and its national transposition) which is enforced (at least in theory) by an equivalent supervision regime. There are some practical issues that make it hard to consistently apply this approach at the European level; however, these are largely smaller problems that can be resolved within the existing legal and trust framework. A series of steps that could be undertaken to address these problems are currently being proposed in the context of the CROBIES study, as will be further noted below.

The second option consists of operating largely on the basis of a contractual framework, which does not depend exclusively on the European regulatory framework and its trust model. By putting in place the appropriate contracts, such service providers can also offer valuable cross border signature validation services with respect to signatures which are not based on qualified certificates, thus potentially giving them a broader scope of application. In this case, the validation service provider defines its own norms and standards, which it applies to any number of chosen CAs, and which it offers to its clients in accordance with their needs. This has the advantage of being applicable internationally (since there is no need to link explicitly to European rules and standards), but it also puts much more effort and responsibility with the validation service provider as a single source of trust (a one stop shop for technical and legal guarantees). From an interoperability perspective, this option also creates the risk that different validation service providers apply different norms and standards, meaning that service providers will not be able to easily compare guarantees offered by different validation service providers.

Thus, the current European eSignatures framework has the potential of supporting eSignature interoperability for signatures based on qualified signatures, since the eSignatures Directive contains a conceptually sound trust framework for such signatures, albeit with certain important issues still to be addressed, which are being examined within the context of the CROBIES study. However, even with respect to signatures based on qualified certificates, there are still a few complicated open questions, including the desirability of a common approach to suitable supervision of CSPs (which is currently a purely national competence), settling the issue of whether a conformity finding by a designated body is needed in order for a signature creation device to be considered a secure signature creation device, and the difficulty of reliable long term validation in the absence of a complete framework for time based signature service (time stamping, electronic archiving, etc.).
With respect to electronic signatures which are not based on qualified certificates, challenges are even greater, especially since the eSignatures Directive doesn't provide a conclusive trust framework for such signatures. Only CSPs issuing qualified certificates to the public are required to be supervised, and while voluntary accreditation schemes can theoretically resolve some of the trust questions for other signature types, such schemes can be freely defined at the national level (meaning they are not equivalent between countries) and are not mandatory. Thus, the EFVS study found that the validation of electronic signatures is confronted with significant barriers, both at the technical, legal and operational level.

The EFVS study examines these questions from the perspective of signature validation at the European level. The CROBIES study on the other hand looks at eSignature interoperability in general, but specifically in the context of cross-border use. While considering a consistent global and long term approach in proposed improvements, CROBIES is also focusing on quick wins that could substantially improve the interoperability of electronic signatures. These include most notably the establishment of a community framework for national Trusted Lists of supervised/accredited CSPs, standardisation efforts in the field of electronic signatures and in particular in relation to certificate profiles, SSCD profiles and signature formats, and the establishment of supervision criteria. However, as CROBIES aims to realise quick wins, it has to rely on the existing framework defined by the eSignatures Directive. As a result, its work faces the same challenges as identified above: its impact can be expected to be substantial mainly with respect to signatures based on qualified certificates but less so for other types of advanced signatures; and certain open issues will still remain.

Whether or not a European framework for the cross-border interoperability of non-qualified signatures is necessary or desirable is of course a policy question, and it was not the aim of this study to take an explicit position with respect to this question. However, when examining European wide eSignature validation problems and how to resolve these (which is the topic of the study), it became clear that many of the relevant questions require a more comprehensive framework than is currently offered by the eSignatures Directive, and this is the case both with respect to signature validation (the EFVS study) and cross border eSignature interoperability in general (the CROBIES study).

Given that the challenges for the EFVS and CROBIES studies are the same, there is an opportunity for convergence between the studies to establish a single coherent strategy to create a comprehensive and consistent framework for eSignature interoperability, by building on the existing European framework for electronic signatures and by filling in the existing blanks in a step by step approach. The goal of the final phase of the study is to present a vision for such a strategy.
2.2 Goals of the present report – addressing identified problems for eSignature validation through a comprehensive framework

This report will try to merge the EFVS and CROBIES work into a broader and consistent vision for European eSignature interoperability, by first taking a step back and looking at existing challenges for electronic signatures in general and signature validation in particular, establishing the steps needed to address these challenges, and then defining a road map to address any remaining issues. The report will be structured as follows:

- **Section 3: Summary of eSignature validation challenges.** In this first section, we will identify the main eSignature interoperability challenges presented by the current situation, followed by an analysis of the strengths and the weaknesses of the current European eSignatures framework. Secondly, we will examine what functionalities we should reasonable expect from a signature validation service provider, and which gaps (legal, technical and trust related) still exist.

- **Section 4: The need for a broader perspective on electronic signatures, signature validation and other CSP services.** This second section examines how an alternative approach could build upon the realisations of the current European eSignatures framework, thus creating a more comprehensive and consistent framework that addresses the challenges for signature validation, and which can be applied to other CSP services as well.

- **Section 5: A roadmap for electronic signature validation.** In this final section, we will examine the steps that need to be undertaken to establish this broader framework, and we will identify the different initiatives already underway that contribute to each of these steps. Finally, we will provide a clear outline on how this approach can conclusively address eSignature validation challenges in the eGovernment context.
3 Summary of eSignature validation challenges

3.1 Current eSignature challenges

3.1.1 Key success factors for eSignatures

Recent surveys, studies and the practical difficulties Member States are encountering when implementing online applications under a number of internal market instruments (e.g. Services Directive, Public Procurement, eInvoicing), show that there is a need for concrete measures to tackle in practice the legal, technical and trust related issues. These measures should include an appropriate promotion and awareness rising to convince the market and business stakeholders of the possible return on investment of electronic signatures.

Key success factors for eSignatures

Realisations, consistency and mapping of efficient Legal, Technical, Trust and Promotional frameworks are key success factors to convince market & business stakeholders of the possible ROI of eSignatures securing their eProcesses.

Sound CSPs & Trust Services
- Provisioning market for interoperable and cross-border use eSignatures
- Promotion

Consistency & formal (efficient) mapping

Sound Legal Framework
- Different level of ES
- Range of ES prod/serv.
- Different types of CSPs
- International dimension

Sound Standardisation Framework
- Covering whole range of ES prod / serv., ES types and types of CSPs
- Business practice driven
- Appropriate guidance
- International dimension

Sound Trust Framework
- Supervision of CSPs
- Voluntary accreditation
- Trust Status Lists
- Application labelling

Figure 1[^2]

[^2]: Graphic taken from the introduction of all CROBIES reports, see [RD3]
Further development and support for interoperable and cross-border electronic signatures in the Information Society should rely on the establishment and/or rationalisation of:

- a **sound and stable legal framework** covering all types of electronic signatures (ES), the whole range of products and services related to electronic signatures, as well as all types of certification services, not limited to the issuance and management of certificates but encompassing any other service using, or ancillary to, electronic signatures, such as time-stamping services, (long term) archiving services, signature validation services, etc., and taking into account the need to include European rules into a worldwide international context;

- a **sound and stable technical & standardisation framework**, covering the above described range of electronic signatures, electronic signature products and services, and certification services in its broader sense, while being business practice driven and providing appropriate guidance and implementation guidelines through international and recognised standards;

- a **sound and stable Trust framework** for both the provision of trusted services and practical implementation of electronic signatures, e.g. through appropriate supervision, voluntary accreditation of trusted services provisioning, as well as certification and/or labelling of electronic signature products and applications;

- the **formal mapping between those frameworks** granting (legal) compliance for those electronic signature products and services which are meeting the relevant requirements;

- the **appropriate education and awareness** around those frameworks,

- consideration of **international and cross-border recognition principles** for a specific set of (qualified) electronic signatures.

The establishment of those sound and stable frameworks and the appropriate and efficient mapping between these frameworks are the **key success factors** to convince the market and business stakeholders of the possible successful implementations of electronic signatures.

Although most of those frameworks are in place today in Europe, there is still room for improvements to reach the right level of maturity and interaction between those frameworks, leading to a successful and interoperable cross-border use of electronic signatures.
3.1.2 Strengths of the European eSignatures framework

Much of the required legal, technical and trust framework (collectively: the European eSignatures framework) exists today, through the eSignatures Directive, its national transpositions, the related standardisation work, and the national trust infrastructure (notably supervision/accreditation schemes) that is being maintained (or in some cases further developed) in connection with the Directive. The basic conceptual approach of the Directive is sound, and it is important to duly recognise these positive elements, in order to appreciate fully which existing eSignature validation challenges can be addressed via the existing framework. Without endeavouring to be exhaustive, the following positive elements should be recognised in particular:

- **Principle of technological neutrality**: the eSignatures Directive is in principle technologically neutral, as it defines its basic concepts (notably electronic signatures and advanced electronic signatures) in terms which do not explicitly refer to any specific technology. The importance of this principle is diminished to some extent due to the fact that other concepts (certificate, qualified certificate, signature creation device and SSCD) are clearly oriented towards a PKI environment. However, the basic scope of applicability of the Directive is linked to the neutral concept of an electronic signature, and the non-discrimination principles of the Directive (article 5.2) build on this. This approach is fundamentally sound, as it ensures that the Directive focuses on a function rather than on a technology.

- **Legal equivalence / legal value**: the Directive takes a two pronged approach to determining the legal value of an electronic signature: for the basic concept of an electronic signature, only the aforementioned non-discrimination principle applies, and the legal value in any proceedings will therefore need to be assessed on a case by case basis. However, for advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device (so called qualified signatures - QES) the legal value is determined by an equivalence rule, declaring such qualified signatures to be legally equivalent to handwritten signatures and by definition admissible as evidence in legal proceedings. Thus, the basic approach is to define a qualified level of the signature, for which specific requirements need to be met that do not necessarily apply to other types of electronic signatures. In return for these specific requirements, a clear legal value is given. This is a positive approach, as it in principle allows similar qualified signatures to benefit from a uniform value across the internal market.

- **Approach to standardisation**: the Directive only defines specific technical requirements at a high and generic level through its Annexes. Details must be fleshed out outside of the legislative process via standardisation procedures, which must then be affirmed and given legal value through a Commission Decision. The fact that technical standards are not integrated into the Directive means that there is greater flexibility in keeping these standards up to date, and ensures that such details can be determined by experts in the field, which should ensure that they are more clearly aligned with the technical state of the art.

- **Supervision and voluntary accreditation**: in order to create a trust framework, it has to be possible for relying parties to confide in the compliance of the electronic signatures with applicable requirements. The Directive allows this via the mandatory supervision of CSPs issuing qualified certificates to the public, and by permitting the introduction of voluntary accreditation schemes. The mandatory supervision scheme is crucial: by ensuring that equivalent supervision schemes are available in each Member States, CSPs issuing such qualified certificates can offer their services from any Member State and in principle be confident that their services will be equally acceptable across the EU. The voluntary accreditation schemes offer Member States to establish separate quality requirements which can further ensure the trustworthiness of specific signature solutions. While this does not have a beneficial interoperability impact at the EU level (since voluntary accreditation schemes are currently established only at the national level, meaning that they are not comparable from one Member State to the next), it should be kept in mind that the main use of such schemes was to create enhanced levels of certification-service provision; not to further enhance interoperability.
- Market access and internal market provisions: the Directive aims to ensure that CSPs can freely establish in any Member State and offer their services throughout the internal market, most notably by explicitly forbidding prior authorization schemes. This ensures that the market cannot be artificially limited or distorted through the introduction of national rules that exclude foreign service providers. This should favour competition, thus leading to improved quality of services and/or lower prices.

- Liability: to ensure that the qualified service level offers real guarantees to relying parties, article 6 of the Directive includes specific liability rules that apply notably to CSPs issuing such certificates to the public, thus ensuring that certain errors linked to the usage of such certificates lead to the liability of a more clearly identifiable party that must assume responsibility for these errors (namely the CSP), rather than allowing all liability to be shifted to a party that may be practically impossible to identify or hold responsible (the signatory). This benefits the trustworthiness of such signatures, and provides the necessary incentive for such CSPs to establish the required processes to ensure the actual reliability of their certificates.

While not exhaustive, the overview above already shows that the Directive has established a conceptually sound approach for the usage of electronic signatures (or at least for certain types of electronic signatures) that should have operated in practice. In the sections below we will examine which elements have not worked out in practice, thus establishing more clearly why interoperability actually remains limited at this time.

### 3.1.3 Weaknesses of the European eSignatures framework

While it is true that with regards to electronic signatures, the basis for those frameworks is in place\(^3\), there are still open issues with regard to the successful, interoperable and cross-border implementation of electronic signatures as depicted in Figure 2 below.

As regards the legal framework, amongst the three forms of electronic signatures defined in Directive 1999/93/EC, only the QES level is (fully) clearly defined and regulated through specific requirements. Similarly, amongst the provision of certification services ancillary to electronic signatures, only the provision of qualified certificates is regulated by Directive 1999/93/EC. There is a lack of common and specific requirements established at the EU level with regards to the provision of other services than the issuance of (qualified) certificates such as e.g. time-stamping, archiving, or eSignature validation. Currently emerging heterogeneous national initiatives may rapidly create or are already creating undesired barriers to cross-border interoperable electronic signatures.

---

\(^3\) Directive 1999/93/EC establishes their legal recognition and a legal framework to promote their interoperability, the technology framework in place is based on a 30-year old mature PKI technology, even more supported by a standardization framework whose establishment followed the Directive implementation through the European Electronic Signature Standardisation Initiative – EESSI – from CEN (www.cen.eu) and ETSI (www.etsi.org).
Status on Key success factors for eSignatures

Commission Decision 2003/511/EC references certain "generally recognised standards" for electronic signature products in compliance with article 3(5) of Directive 1999/93/EC which, when they are complied with, grant presumption of compliance with the requirements in the sole Annex II.(f) and Annex III of Directive 1999/93/EC. No formal mapping between other legal requirements related to the use of electronic signatures and the current 30+ standardisation deliverables from the existing EU eSignature standardisation framework is available.

Despite some successes, the eSignature standardization work initiated after the adoption of Directive 1999/93/EC has resulted in a complex European eSignature standardisation framework lacking business orientation, clear standards or norms, international dimension, and implementation guidelines. Such an inappropriate standardisation framework also contributed to the current lack of interoperable cross-border eSignature applications. There is an urgent need for some significant rationalization work which will be addressed by the freshly issued Mandate M/460 [RD5] to the ESOs in line with the European Commission eSignature and eIdentification Action Plan [RD4] and supported by the CROBIES study inputs [RD3].

On the Trust framework level, no common minimum requirements support the mutual recognition of the Member States’ supervision system of certification service providers issuing QCs, since Directive 1999/93/EC allows Member States to decide what they consider an appropriate supervision system. All the existing CSPs issuing QCs, a little more than 100, supervised or accredited in 23 Member States out of the 27 Member States are listed in the national Member States’ List in which they are established or accredited. Until recently, one could...
observe a wide diversity in the information provided in such lists, with some lists stating only the registered name of the supervised/accredited CSP issuing QC and other lists containing very detailed information per issuing CA service from supervised/accredited CSPs. Still the majority of those lists did not provide sufficient information to fully support the validation of QES or AdES QC. The common template for Member States Trusted Lists of supervised/accredited CSPs and the related Member States obligations stated in Commission Decision 2009/767/EC [RD6] will ensure that a sufficient and homogeneous baseline of information is available for all of these CSPs.

Furthermore no real consistency exists between the different aspects of e-Signatures (legal, standards and trust related), and no or extremely poor promotion is given to the interoperable and cross-border use of electronic signatures.

Considering the current situation, even if most of the basic elements of the required framework are in place, one is however quite far from an ideal situation of sound, consistent and efficient frameworks fully supporting the eSignatures market and its stakeholders.

However, leveraging the recent significant steps and looking for convergence of the associated Action Plan on e-signatures and e-identification [RD4], studies\(^6\), the ICT PSP pilots\(^7\) and other activities, it is opportune to establish a single coherent strategy to create a comprehensive and consistent framework for eSignature interoperability, by building on the existing European framework for electronic signatures and by filling in the existing blanks in a step by step approach.


\(^7\) Specifically STORK (https://www.eid-stork.eu/), PEPPOL (http://www.peppol.eu/) and SPOCS (http://www.eu-sposcs.eu/)
3.2 Specific challenges for eSignature validation

In the earlier stages, the challenges for eSignature validation at the European level have been extensively examined. The section below will summarise (1) what functionalities should be provided by an ideal signature validation service provider; (2) what each of these functions entails, and who/what is involved; and (3) what the main challenges for signature validation are.

3.2.1 Describing an ideal signature validation solution

In the earlier EFVS reports, the services to be provided by a signature validation service were already examined, and the position was taken that at a minimum these should include the validation of signature certificates (both technical validation and assessment of their quality), signature validation as a whole (again including technical validation and assessment of quality), and, to distinguish validation services from validation authorities, the need for the latter for some form of liability model. In addition, it was noted that certain additional services may be required to attach consequences to the signature, including semantic services and historical validation services. The graphic below provides a more systematic overview of these services, functionalities and stakeholders involved.
Figure 3

Legend:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSP</td>
<td>Certification Service Provider</td>
</tr>
<tr>
<td>VSP</td>
<td>Validation Service Provider</td>
</tr>
<tr>
<td>CSP</td>
<td>Certification Service Provider</td>
</tr>
<tr>
<td>TSSP</td>
<td>Time Stamping Service Provider</td>
</tr>
<tr>
<td>LTASP</td>
<td>Long Term Archiving Service Provider</td>
</tr>
<tr>
<td>SP</td>
<td>Signature Policy Service Provider (Signature Policy Issuer)</td>
</tr>
<tr>
<td>Id°SP</td>
<td>Identification Service Provider</td>
</tr>
<tr>
<td>Au°SP</td>
<td>Authentication Service Provider</td>
</tr>
<tr>
<td>LT</td>
<td>Signature Policy</td>
</tr>
<tr>
<td>TSL</td>
<td>Trust Status List</td>
</tr>
<tr>
<td>TL</td>
<td>Trusted List (as defined in Commission Decision 2009/767/EC [RD6])</td>
</tr>
<tr>
<td>LOTL</td>
<td>List Of The Lists</td>
</tr>
</tbody>
</table>

Globally, the following logical structure exists in the usage of electronic signatures (including their validation):

- Signatories create signatures, with the purpose of authenticating a document so that the signature can later be validated by a relying party and potentially within the expression of some commitment with regards to the signature.

- In order to validate a received electronic signature, a Relying Party needs to rely on the services of trust service providers (TSPs), as neutral third parties trusted by both the signatory and the relying party. The CA (who issues the signature certificate to the signatory and is liable for the certificate validity status information) is an obvious and necessary example of such a TSP. However, other TSPs may also be involved, with examples in the above Figure 3 including e.g.
  - time stamping authorities, since there may otherwise not be a reliable way to determine when or before when a signature was created, and therefore also no reliable way to determine whether it was valid at the time of signing/verifying or at the time the validation must relate to;
  - long term archiving authorities, ensuring that the signature and/or signed document can be validated or read over a longer period of time, thus acting as a guardian against deprecation;
  - signature policy authorities who issue signature policies used to determine the exact conditions under which a signature must be created and verified before it can be considered as valid in a given context.

Validation service providers are another class of TSPs, who can offer any or all of the services above as a single point of contact (either by offering those services itself, or by relying on external TSPs), thus making easier and more efficient for relying parties the validation of electronic signatures.

- TSLs can be used to identify TSPs which meet specific requirements that are considered crucial in a specific context. With respect to CAs, the Trusted Lists [RD6] created and maintained at the national level by supervisory bodies are one such example; however, it is certainly conceivable that lists for other TSPs would be created and maintained by other governance bodies (including private sector parties, if appropriate), and that they would be created at a sector specific level (e.g. VAs which are considered appropriate for eGovernment or eBanking purposes), rather than at a geographic level like...
the national TSLs of CAs. These TSLs serve a crucial transparency and interoperability purpose, since they allow relying parties to easily determine whether a TSP respects a consistent set of requirements.

In the section below, the stakeholders, functionalities and services will be more systematically described.

### 3.2.2 Defining the building blocks, services and stakeholders

Based on the logical model described above and on the experiences derived from the eSignatures Directive, it is possible to establish a more neutral set of definitions of the key building blocks, services and stakeholders described in the graphic. While the definitions are based on those of the Directive, where necessary they have been broadened to ensure their applicability to TSP services in general, rather than restricting it to electronic signatures *sensu stricto*. These tentative definitions are provided below.

- **‘Certificate’** means, as defined in Article 2.9 of Directive 1999/93/EC [RD1], an electronic attestation which links signature verification data to a person and confirms the identity of that person.

- **‘Certification Service Provider’** means, as defined in Article 2.11 of [RD1], an entity or a legal or a natural person who issues certificates or provides other services related to electronic signatures.

- **‘Certification Authority’** means a CSP issuing digital certificates. A CA can use several technical CA’s private keys, each having an associated certificate, in order to issue end-entity certificates. A CA is an authority trusted by one or more users to create and assign certificates. Optionally the Certification Authority may create the users’ keys [ETSI TS 102 042]. The CA is deemed to be identified through the identification information present in the Issuer field of the CA certificate related to (certifying) the public key associated to the CA’s private signing key effectively used by the CA to issue entity certificates. A CA may have several signing keys. Every CA signing key is uniquely identified by a unique identifier as part of the Authority Key Identifier field in the CA’s certificate.

- **‘Trust Service Provider’** means an entity or a legal or natural person who provides one or more (electronic) Trust Services meaning services which enhances trust and confidence in electronic transactions (typically but not necessarily involving cryptographic techniques or confidential material). In the context of the present document we address mainly TSP providing services ancillary to electronic signatures (also defined as CSP in [RD1]) covering CSPs issuing (qualified and/or non qualified) certificates, CSPs providing services supporting electronic signatures (e.g. Timestamping services, eSignature Validation services, (Long Term) Archiving services, signature policy authority services, Identification Authority (Id°A) services and Authentication Authority (Au°A) services), and CSPs providing service employing electronic signatures (e.g. Registered mail services).

- **‘Signature Verification Data’** means, as defined in Article 2.7 of [RD1], data such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

- **‘Signature Creation Data’** means, as defined in Article 2.4 of [RD1], unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

- **‘Signature Creation Device’** means, as defined in Article 2.5 of [RD1], configured software or hardware used to implement the signature creation data.
‘Signatory’ means, as defined in Article 2.3 of [RD1], a person who holds a signature creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents. Note that ‘person’ is defined and interpreted according to Member States’ national laws.

‘Validation Service Provider’ means a CSP offering the following services in relation to electronic signatures supported by signing certificates issued by independent CAs:

a) **Validation of the signature certificate(s)**, including notably
   i. The validation of the CA’s signature on the signatory’s certificate for authenticity and integrity verification purposes;
   ii. The validation of the validity and non-revocation of the signatory’s certificate;
   iii. The validation of the quality of the signatory’s certificate against some quality criteria (e.g. as part of a Signature Validation Policy, on request of the validation service user or as defined by the validation service).

   Note: This validation step should be extended to include the certificate chain, starting from the signatory’s certificate up to a trusted (root) CA certificate.

   iv. (Extended service) Semantic services e.g. with regard to the identity of the signatory, its legal capacity or its location.

b) **Validation of the electronic signature**, including notably
   i. The technical validation of the electronic signature depending on the multitude of possible formats and algorithms that may be in use;
   ii. The validation of the quality of the signature (on technical aspects) against some quality criteria (e.g. as part of a Signature Validation Policy, on request of the validation service user or as defined by the validation service);
   iii. (Extended service) The technical completion of the electronic signature according to the submitted electronic signature data and form. This may include but not limited to all or a combination of the following:
      a. Applying a Trusted Time Attribute on the signature data (e.g. a trusted time stamp or a trusted time mark);
      b. Adding complete validation data references and/or values (i.e. references to or values of all the certificates present in the certification path used for verifying the signature) and the complete revocation references and/or values (i.e. references to or values of the CRLs and/or OCSP responses used for verifying the signature);
      c. Applying a Trusted Time Attribute (e.g. a trusted time stamp or a trusted time mark) on the validation data references and revocation references;
      d. Adding an Archival Trusted Time Attribute on the completed electronic signature form as per above a, b, c items.

Note on a) and b): The notion of time is of crucial importance in the context of signature validation and signature certificate validation. It covers the time to which the signature creation is claimed to be associated, believed or trustworthily associated, the time to which the certificate validity status information can be reported and the time to which the validation process is to relate, being current or in

---

8 This chain from the signatory certificate up to a trusted CA anchor is defining a certification path.
the past. This renders “historical validation services” intrinsically linked to basic services when considering signature certificates and signature validation services.

c) **Extended services:** This may optionally include but not limited to the following ancillary services

i. Trusted Time services (e.g. Time-stamping services, Time-marking services);

ii. (Long term) Archiving of the signatures and/or signed documents;

iii. The maintenance of the signature/document formats;

iv. Any additional transactional service or delivery service related to the signed documents and signatures;

The basic services as listed above (those not marked as *extended services*) are considered to be crucial when meeting the above definition (i.e. to determine whether or not a TSP can be considered a VA).

d) ‘**Validation Authority**’ means a Validation Service Provider which additionally provides end-users with specific **guarantees with regard to the trustworthiness and legal reliability** of the electronic signature, i.e. assessing the legal value of the signature and providing an acceptable liability model that allows the relying party to rely legally on this statement. Such guarantees can rely on statements made on some technical or legal requirements and/or quality criteria on certificates and electronic signatures. This may involve all or a limited combination of the following:

- **Type of electronic signature** (e.g. qualified electronic signature, advanced electronic signature supported by a qualified certificate, advanced electronic signature);

- **Timing constraints and sequences** (e.g. with regards to the certificate(s) and/or the electronic signature);

- **Rules for the use of Trusted Time facilities (in compliance with timing constraints and sequences)**;

- **Signatory identification rules including** e.g. roles, attributes or associated proof of authority, confirming the legal capacity of a signatory);

- **Rules for the use of Certification Authorities (in compliance with the signatory identification rules)** e.g. confirmation that the certificate is qualified in the sense of Directive 1999/93/EC, confirmation that certificate has been issued according to some policy requirements prescribed by the VA services end-user or by the VA itself for example simply relating to the fact that the CA originates from a set of pre-approved CSPs, including e.g. CAs which are featured on a specific TSL)

- **Rules for the use of certificate validity status information** (e.g., CRLs, OCSP);

- **Rules for creating a complete certificate chain up to a trusted Certification Authority**;

- **Rules related to the use of signature commitments**;

- **Rules on the strength of the signature creation and other security considerations** (e.g. strength of the signature cryptographic suite, namely constraints on the signature algorithms, key lengths, hashing function, and parameters);

- **Rules on the signature verification data to be provided by the signatory and/or collected by the verifier**;

- **Rules on the Long Term Validity management of the validated electronic signature**;

- **Classifying the certificate and/or the electronic signature as a whole according to some criteria system** (this latter can be prescribed by the VA service end-user, standardized or defined by the VA);

Those elements can rely on a Signature Policy, i.e. a set of rules for the creation and validation of an electronic signature under which the signature can be determined as valid and the outputs of applying
those rules while validating an electronic signature. A Signature Policy can be either explicit or implicit, be defined by the VSP or the relying party using the VSP services or jointly negotiated by the parties.

- ‘Validation Service’ means a service provided by a Validation Service Provider.

- ‘Signature Policy’ means a set of rules for the creation and validation of one or more interrelated electronic signatures that defines the technical and procedural requirements for creation, validation and (long term) management of this(these) electronic signature(s), in order to meet a particular business need, and under which the signature(s) can be determined to be valid.

Note: A Signature Policy covers the three following aspects related to the management of each of the considered electronic signatures:

1) **Signature Creation Policy**: part of the signature policy, which specifies the technical and procedural requirements on the signer in creating a signature;

2) **Signature Validation Policy**

3) **Signature (LTV) Management Policy**: part of the signature policy, which specifies the technical and procedural requirements on the long term management and preservation of a signature.

- ‘Machine Processable Signature Policy’ [RFC 3125, ETSI TR 102 272 & 102 038]: The Signature Policy Issuer (which is a Trust Service Provider (TSP)) issues signatures policies that define the technical and procedural requirements for electronic signature creation, and validation/verification, in order to meet a particular business need. The signature policy is a set of rules for the creation and validation of an electronic signature, under which the signature can be determined to be valid. Signature policies, and in particular MPSP compliant with e.g. RFC 3125 should contain general information including a unique identifier of the policy, the name of the issuer, the date of issuance, its field of application and one or more Signature Validation Policies expressed according to the RFC 3125 specifications.

In summary, and as in earlier EFVS reports, for the purpose of this document the VA is defined as a CSP providing at a minimum the three services of validation of signature certificate(s), of validation of signatures, and of assuming liability with regards to the trustworthiness and legal reliability of the validated electronic signature. Those services can be provided in their basic or extended form (e.g. including some semantic services or services related to the long term validity of the validated electronic signatures). Assuming responsibility towards the end-user is the criterion to distinguish between a validation service (a technical concept) and a validation

---

9 Those definitions (above and below) slightly differ from but further precise the definitions provided in ETSI related standards (ETSI TR 102 041, 102 045, 102 038, 102 272) and RFC 3125. Those cited standards being either incomplete, not finalised or outdated, their review is expected to be part of the standardisation efforts in the context of the m460 mandate [RD6].

10 Of course the Signature Creation Policy and Signature Validation Policy should correspond to each other.
authority service (a service with legal value). The validation service is defined as a solution that essentially consists of the dissemination of information regarding the output of the service (e.g. information regarding the certificate validity, quality and CA practices, information about the technical validation of the signature, quality and signature creation/validation practices) which the end-user can then choose to rely at his own risk.

It is clear that the description above also features a number of concepts which have not yet received much attention yet at the European level, including the set of rules being used by the VA when validating an electronic signature at the request of an end-user and under which the signature can be determined to be valid. Such a set of rules is commonly designated as a Signature Policy. Such a policy can be either defined by the relying party requiring the services from the VA, or by the VA itself or jointly by the VA and the Relying Party.

As a corner stone of such set of rules, and of the validation process of electronic signatures, the need for a standardized definition of quality criteria with regards to the electronic signature and its supporting signature certificates is of crucial importance when considering interoperability and cross-border validation of electronic signatures. This is one of the remaining challenges for signature validation service providers\footnote{\textsuperscript{11}}, as will be further examined below.

### 3.2.3 Current challenges for signature validation service providers

Existing challenges for signature validation service providers wishing to operate at the European level have been identified in previous EFVS reports, and comprise notably the following points:

#### 3.2.3.1 Legal gaps

##### 3.2.3.1.1 Defining a validation service provider

The sections above provided a summary indication of the functionalities involved in establishing and operating a signature validation service provider. However, this overview is based on the analysis performed within this study, and has no legal basis. From a legal perspective, the concept of a validation service provider is entirely undefined, meaning that their services are not comparable at the European level, and that specific requirements and legitimate expectations are impossible to determine uniformly.

##### 3.2.3.1.2 Defining ancillary services

The same problem applies also to any number of ancillary services that may be used by the VSP: time stamping, long term archiving, signature policy issuers, etc. Each of these may be an important component in the VSPs services, yet a legal framework that fixates their obligations is virtually completely absent.

##### 3.2.3.1.3 Assessing the trustworthiness of CAs covered by the validation service

The issuing of determining the trustworthiness of CAs is of course not purely technical in nature. While the eSignatures Directive introduces the notion of a CSP issuing qualified certificates to the public, no further distinctions are made between CAs or the guarantees that they provide. As a result, existing validation service providers have to establish their own criteria, leading to market fragmentation. This impairs cross border service provision, at least with respect to signatures which are not based on qualified certificates.

\footnote{\textsuperscript{11} Note that this should be extended to any type of Trust Service Token being the result of the provision of a Trust Service.}
3.2.3.1.4 Security levels – legal qualification of certificates and signature types

From a trust perspective, one of the most complicated issues is determining the quality of the signature certificate being used and the signature created with this certificate. From a legal perspective, the European regulatory framework essentially offers only two major reference points: a signature certificate is either qualified or not qualified, and an electronic signature can be either qualified (or using the legal terms of the Directive: an advanced signature created using a qualified certificate and a secure signature creation device or SSCD) or nonqualified. It is therefore not surprising that two of the key VA solutions studied in previous reports use only this distinction, and cannot make any judgments on the quality of signatures that do not use qualified certificates (or on nonqualified certificates as such).

Strictly speaking this does not need to be a problem, especially in environments where qualified certificates are relatively abundant and commonly used. However, this description is certainly not applicable to the whole of the European market as it stands. In this respect, an acceptance that European validation service providers will only be able to make any statements in relation to the quality of qualified certificates and/or qualified signatures may be seen as being out of phase with market realities. It would be desirable for validation service providers to have a wider range of options open to them, as this would be beneficial to the interoperability of nonqualified signature solutions, without any impact on the interoperability of qualified signatures.

3.2.3.1.5 Responsibility and liability

One of the main reasons why foreign signatures cannot easily be accepted in eGovernment applications is the current impossibility of obtaining sufficient guarantees with regard to the reliability and value of such signatures, backed by an entity willing to take responsibility and liability for making assertions related to this point. Of course, this is one of the main reasons for relying on a validation service provider: the possibility of outsourcing this difficult exercise to a qualified and trusted third party.

However, due to the absence of a coherent legal framework for signature validation service providers, it is also unclear which guarantees they provide, or what criteria VSPs should be using to determine whether or not a CA (other than those issuing qualified certificates to the public, which are covered by the Directive in sufficient detail) is indeed trustworthy or not.

3.2.3.2 Technical gaps

3.2.3.2.1 Signature Type – SSCD status

Establishing when a signature can be accepted as a Qualified Signature is difficult in practice. This is caused by the fact that Qualified Certificates Statements "qCStatements extension" as defined in the RFC 3739 is optional and not (yet) systematically used. Perhaps more importantly, there is no clear way at this time to establish if the signature creation device that was used by the signatory can be considered an SSCD in the sense of the Signatures Directive. Thus, especially at a cross border level, it is very complicated to identify qualified signatures as such. This issue is being examined within the context of the CROBIES study, specifically the aforementioned efforts related to the establishment of national trusted lists of supervised/accredited CSPs issuing qualified certificates to the public. The resulting national lists should prove a highly useful resource in addressing this issue. However, settling the discussion on whether formal conformity assessments by designated bodies is necessary before a signature creation device can be considered an SSCD under the Directive will likely require further action beyond CROBIES.

3.2.3.2.2 Signature format

Having multiple types of signature formats in use across Europe constitutes an interoperability barrier if the signature has to be verifiable in multiple Member States. While overcoming such differences is one of the core functionalities of a VSP, it is clear that a multitude of formats complicates the field significantly.
This issue is also being examined within the context of the CROBIES study, specifically by examining the possibility of harmonising existing signature formats for the public sector.

3.2.3.2.3 Validation protocols

In order to perform a signature validation, relying parties must be capable of communicating with their VSPs, and in a federated validation infrastructure (as has been examined in previous reports) VSPs need to be able to communicate between themselves as well. In the previous reports, we have seen that a number of solutions are available (Web services, OASIS-DSS, XKMS, DVCS), but there is no ‘standard’ approach that VSPs can conform to. Thus, while specific standards are available, implementation is still very different from VSP to VSP.

3.2.3.2.4 Semantic interpretation of certificate fields

There is a lack of consistency in the semantic interpretation of certificate fields within various digital certificate implementations. Not all European CAs give the same meaning to the same certificate fields. Therefore, it is currently up to each VSP to develop ad-hoc parsing services, specific OCSP/CRL connections where applicable and/or ad-hoc syntax and semantic checks of certificates. Further guidance in this respect appears to be needed.

3.2.3.3 Trust gaps

3.2.3.3.1 Trustworthiness of the VSP

For CAs, a certain trust infrastructure was established via the eSignatures Directive, since specific requirements were defined for CAs issuing qualified certificates to the public, and since the compliance with these requirements is supervised at the national level through supervisory bodies. In this manner, a relying party can determine the trustworthiness of these CAs by checking their supervision status. However, as was noted above, similar requirements are not available for VSPs, and no supervision regime exists. Therefore, the trustworthiness of a VSP must be determined by its customers on a case by case basis. There is a need for suitable requirements, as well as for conformity assessment guidance for evaluating and assessing compliance with relevant requirements.

3.2.3.3.2 Trustworthiness of TSPs used/covered by the VSP

To provide its services, the VSP needs to establish appropriate processes for determining the reliability of any covered CAs. If the VSP only wishes to make a statement on whether or not these CAs are issuing qualified certificates to the public, the European framework is appropriate. However, for other types of CSPs, no suitable criteria are available, meaning that each VSP must do this exercise on its own, using its own set of criteria. Obviously, this is a barrier to cross border interoperability.

However, it is important to note that CAs are not the only type of TSP with which the VSP is likely to have a business relationship. As was explained above, the VSP may also rely on TSPs for time-stamping purposes, on SPAs for the definition of signature policies, on LTAAs for long term archiving services, etc. The same problem applies in each case: no criteria exist to determine their trustworthiness at the European level, nor any conformity assessment guidance for evaluating and assessing compliance.
Thus, if comprehensive signature validation services (i.e. also covering signatures other than those based on qualified certificates) are to be developed, then it is clear that there is a need for a common European definition and metrics for quality criteria of:

- Certificates other than qualified certificates
- Electronic Signatures other than qualified signatures
- Other Trust Service Tokens (e.g. Time stamp tokens, Signature Policies, Long Term Archives) which may be needed or beneficial to support the actual usage in practice of electronic signatures.
4 The need for a broader perspective on electronic signatures, signature validation and other CSP services.

4.1 Introduction

Prior work in the EFVS study aimed to identify how signature validation services are presently operating in Europe, and how a validation service could be designed (possibly using a federated model) in a way that would be valid and usable in all of the EU, and that would also be able to cover signatures which are not based on qualified certificates. However, and as summarised in the overview above, a key conclusion of the preceding work was that there are challenges that cannot be resolved under the present eSignatures framework, due to the fact that certain crucial issues in the legal, technical and trust framework are not dealt with. While it is possible for validation service providers to design their own solutions – as is presently being done – these services can only operate on a local basis, as a solid European level foundation for all aspects of their services is simply missing. The role of a signature validation service provider is not regulated in a comprehensive manner, the standards that they should apply are incomplete or lack a European standing, and the trust framework can only be established on an ad hoc basis. In this environment, comprehensive and durable signature validation solutions with a general EU level impact are virtually impossible to design.

It may therefore be worth examining how the existing framework – the Directive, standards and trust framework - can be recast in a broader and more comprehensive form in the future, in a way that would address the present challenges for signature validation service providers while respecting and building on the progress made so far in the field of eSignature interoperability, and even extended to a complete Identification Authentication Signature policy. This recasting should:

- Build on the numerous positive aspects of the Directive (technology neutral, internal market provisions, supervision approach etc., as described above);
- Use the approach of the eSignature Directive business model of mapping functional legal requirements to generally recognised standards when such a model has been fully implemented (for CSPs issuing QCs);
- Fully respect existing solutions and investments due to its re-use of these positive elements (it is a recasting; not a rebuilding from scratch);
- Aim to remedy the aforementioned shortcomings (incomplete trust model, ambiguities etc);
- Examine how the general model of the eSignatures Directive can be opened up to cover other contexts, thus establishing the missing links to ancillary services.

In the section below, the EFVS/CROBIES team will provide its general reflections on what an optimal and comprehensive normative framework might look like. We believe that the envisaged framework would be capable of handling the eSignature validation challenges, and could create a real added value in other areas as well, serving as a more consistent and encompassing solution than the present eSignatures Directive, ultimately addressing fully the Identification, Authentication and Signature policy issues.
4.2 eSignatures, eSignature validation and other TSP services

It should be clear from the previous study deliverables and in particular also from Figure 3, that eSignature validation services are only one type of TSP services, and that many of the problems identified for such services exist for other TSP services as well, and that the solutions are similar.

Certain challenges have been identified that would be impossible to resolve by relying purely on the eSignatures Directive, as they are simply not under its present scope. It may be therefore worth examining how the legal framework for eSignatures could be updated to ensure the comprehensiveness of the model, i.e. by recasting the existing Directive into a newer version that applies to TSP services in general. The EU could choose to regulate this, since it is clearly an internal market issue, in precisely the same way that the eSignatures Directive was: the current lack/ inadequacies of a European framework is causing market disruptions which would be hard to address conclusively without further European intervention. It should thus be stressed that we are treating the issue as such: as existing technical services in need of a comprehensive framework that should be harmonised across the EU to minimise barriers to the internal market.

As also stressed in the CROBIES study, we would recommend extending the scope of Directive 1999/93/EC, through any appropriate means, in order to integrate specific requirements on the provision of certification services other than issuing qualified certificates to the public, focusing on services ancillary to electronic signatures. Currently, Directive 1999/93/EC already affects all types of certification services ancillary to electronic signatures, notably via the concepts of certification service provider (‘an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures’, Art.2.11) and of electronic-signature product (‘hardware or software, or relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures’, Art.2.12).

Neither of these concepts is restricted to only CSPs issuing qualified certificates to the public. Their general scope is again stressed in recital 9, noting that ‘Electronic signatures will be used in a large variety of circumstances and applications, resulting in a wide range of new services and products related to or using electronic signatures; the definition of such products and services should not be limited to the issuance and management of certificates, but should also encompass any other service and product using, or ancillary to, electronic signatures, such as registration services, time-stamping services, directory services, computing services or consultancy services related to electronic signatures’.

Art. 3.5 of the Directive allows the Commission to establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal. In this way, it can be argued that the Directive already allows the Commission to impact the activities of CSPs other than those issuing qualified certificates to the public (although admittedly there would be no discernable binding legal consequence to CSPs other than those issuing qualified certificates to the public or to SSCDs, due to article 3.5’s link with Annex II and III). This would cover amongst others:

- CSPs issuing (qualified or non qualified) certificates;
- CSPs providing services supporting electronic signatures (e.g. Timestamping services, eSignature Validation services, (Long Term) Archiving services);
- CSPs providing services employing electronic signatures;
• And to be more complete, this should also encompass Identification Authority (Id°A) services and Authentication Authority (Au°A) services.

However, the detailed requirements and annexes of the Directive focus on one specific type of CSP, namely a CSP (or perhaps more accurately a CA) issuing QCs to the public. Currently, this is de facto the Directive’s main area of focus by design, and the impact or consequences of the Directive for other types of CSPs (including CSPs issuing non-qualified certificates or time stamping service providers) appear to be very limited: e.g. the obligations and liabilities of other types of CSPs are undefined.

The lack of detailed requirements for other types of certification services ancillary to electronic signatures has lead some Member States to establish national laws and regulations on the provision of such services. E.g. Italy, Germany and Hungary, amongst others have national laws on the provision of time-stamping services in particular when supporting (qualified) electronic signatures.

Divergences in such national laws may rapidly create new barriers to the interoperable and cross-border use of electronic signatures. E.g. to have a long term electronic signatures equivalent to hand written signature valid in the Community, it may be required to implement as many time-stamp tokens as there are divergent national regulations in the EU. This is a serious barrier to the deployment of such services at an EU wide level.

Establishing a common framework applicable to all types of certification services is not only strongly recommended but is an essential action with regards to the facilitation of the interoperability and cross-border use of electronic signatures beyond QES and AdES QC. Similarly, defining levels of (other than Qualified) advanced electronic signatures and associated certification security/quality/policy levels for supporting digital certificates is equally important. The identification and definition of the certification services, their component services and the associated categorisation in terms of security/quality/policy levels would be a critical starting point for establishing a common framework for legal requirements for those services. The legal effect and value of the resulting certification services outputs should also be carefully defined and clarified.

Even when focusing exclusively on eSignature Validation Services, the above proposed approach (covering a much wider variety of TSPs) is believed to be the sole alternative due to the strong dependence of the VSP services on other Trust services ancillary to electronic signatures (as depicted in Figure 3). To solve existing VSP questions, an answer must also be found for the (largely similar) issues present in all those other Trust services.

In the sections below, we will explore how such a framework could be formed. As will be seen, many of the building blocks are already in place, and the main challenge is to extend and reshape these into a coherent whole.
4.3 Conceptual model for a rationalised and comprehensive eSignature framework

4.3.1 From a legal perspective

In the sections above, we already noted that the eSignatures Directive has a number of clear strengths that can certainly be built on and should be retained in a future legal framework, including:

- The principle of technological neutrality;
- The legal equivalence / legal value rules;
- Its approach to standardisation;
- The supervision and voluntary accreditation mechanisms;
- Its market access and internal market provisions;
- The liability approach.

While a number of smaller weaknesses can be identified on some of these points in the present Directive, the general model could certainly be retained and reshaped for a broader context, i.e. covering VSPs and other ancillary TSPs needed to create a comprehensive legal eSignatures framework.

Broadly speaking, the model for such a TSP Directive should be structured around three main pillars:

- A common section, which acts as a general framework applicable to any TSP service. This will include the general definition of the strengths noted above, and ensure that they will be defined for specific types of TSP services.
- A service specific section, where the characteristics and requirements for each service are defined separately. One could e.g. envision that this section would contain a subsection on e.g. CA services (largely comparable to the current eSignatures Directive), a subsection for VSPs, for TSPs, for LTAAs, etc.
- Finally, technical details such as specific quality requirements which are reliant on standardisation would be addressed outside of the Directive, via Commission Decisions, as with the present Directive.

Thus, the common section would act as a framework for all TSP services. It would contain notably:

- A definition of the concept of a TSP service, and of specific TSP services (eSignatures, timestamping, electronic archiving,...) to be covered by the Directive.
- The principle that all TSP services will exist in two varieties: qualified and non-qualified. As with the eSignatures Directive, non-qualified TSP services will benefit from non-discrimination rules; while qualified ones should get a specific legal value that applied in any Member State (e.g. for qualified time stamping services an irrefutable legal presumption of the correctness of the exact time at the moment of time stamping could be introduced). Thus, the same approach that already exists for eSignatures would also be applied to other types of TSP services.
• A supervision and accreditation framework: each TSP service *has* to be supervised if it is qualified; it *may* be accredited if it is non-qualified. Supervision has to follow EU standards, while accreditation can be done in accordance with EU standards or in accordance with context specific (e.g. national) standards. If EU level accreditation standards are followed, then they will be interoperable EU-wide; otherwise no interoperability is guaranteed.

• A framework for the adoption of standards for TSP services via Commission Decisions, as in the current Directive.

• General internal market rules.

Specific TSP services (like those in the list above) would be regulated through the service specific section. Each service would be governed through a specific subsection containing:

• The legal effect of the qualified TSP service (e.g. the equivalence to a hand written signature for qualified signatures);

• Liability rules and internal market rules if they differ from the common section. To determine appropriate rules with respect to liability (i.e. to answer the question what a given TSP is liable for), the link with supervision/accreditation schemes would be a natural and logical starting point. In the present state of affairs, the eSignatures Directive only defines minimum liability rules for CSPs issuing qualified certificates to the public (article 6); for other types of CSPs (including those issuing nonqualified certificates to the public), no similar liability rules are made explicit in the Directive. In a future revised legal framework for TSP services, any TSP who is subject to a mandatory supervision regime or who voluntarily joins an accreditation scheme could be made liable towards any relying third parties for its compliance with any requirements imposed by that supervision/accreditation scheme. In this way, the reliability of foreign TSPs could be more easily determined if they are supervised or accredited, on the basis that the relying party can count on these TSPs being liable for their compliance with any imposed requirements. In this way, a certain degree of liability could also be logically attached to nonqualified TSPs.

It should be noted that the question of liability is thus separate of that of the legal effect of a service. E.g. for electronic signatures, it seems likely that the current arrangement with respect to the legal value of electronic signatures (equivalence for qualified signatures, non-discrimination for all signatures) would remain the same at the European level; the creation of additional levels of signatures would not imply that other some of those levels would also have to be made equivalent to handwritten signatures at the European level. It only implies that it should become easier to determine the reliability of those eSignatures, allowing relying parties to determine whether they consider them to be acceptable for their purposes, keeping into account their national rules and local policies and preferences. Automatic equivalence imposed at the European level would remain restricted to the qualified service level.

Applicable standards could be identified by referencing them. A clear mechanism should be organised to ensure the clear mapping between those legal requirements and provisions and the standardisation framework, being related to the technical specifications and policy requirements to be implemented by the TSPs, along with clear Conformity Assessment Guidance to be used by evaluators to assess the compliance of such services to the relevant requirements and on the basis of which supervision and voluntary accreditation models could be established in a coherent manner.
4.3.2 From a technical perspective

As was noted above, the existing standardisation framework for eSignatures is outdated, incomplete and inaccurate, and for other TSP services a relevant European standardisation framework is missing entirely. However, the European eSignature standardisation framework is soon to be rationalised in the context of the European Commission Mandate M/460 addressed to the ESOs [RD5]. Given the considerations presented in this document, it is strongly recommended for these efforts to be actively driven in the direction of supporting a recast legal framework as proposed above.

The resulting EU rationalised European Electronic Signature Standards (EESS) [RD5] should be targeting the production of three main types of results:

- Technical specifications and policy requirements on the basis of which TSPs can base the developments, set-up and production of their services;
- The Conformity Assessment Guidance (CAG) on the basis of which the verification of conformity of TSP services, electronic signature products, systems and services that implement the standards can be performed, and on the basis of which supervision and voluntary accreditation systems can be built;
- Implementation guidelines giving support for the cross-border interoperability, providing guidance and efficient implementation of the standards.

As already stressed in Mandate M/460 [RD5], the architecture of the rationalised EU eSignature standardisation framework should be organised around the following eSignature products and services categories:

- CSPs issuing (qualified and/or non qualified) certificates;
- CSP services other than issuing certificates
  a) CSPs providing services supporting electronic signatures (e.g. Timestamping services, eSignature Validation services, (Long Term) Archiving services, signature policy authority services); and to be more complete, this should also encompass Identification Authority (Id°A) services and Authentication Authority (Au°A) services;
  b) CSPs providing service employing electronic signatures (e.g. Registered mail services);
- Secure Signature Creation Devices;
- Products related to the creation and/or validation of electronic signatures.

In particular the following specific standardisation actions are required and considered as crucial in the present context:

- Common definitions of the above products and services, in particular TSP services, as well as those of the various types and variants under which they may be operated, is of crucial importance when ensuring interoperability and cross-border use of such products and services.
- Commonly defined identification elements (e.g. (sub)type identifiers) for those kinds of products and services are crucial when aiming to identify to which category(ies) a determined service belongs and is accordingly granted a potential approval status according to whatever approval scheme.
- The establishment of quality criteria for certificates and electronic signatures\(^{12}\), as well as for other Trust Service Tokens e.g. digital certificates, time stamp tokens, long term archives, signature policies, etc.
- The rationalised profile for Qualified Certificates\(^{13}\) and non-Qualified certificates.
- A common identification profile for signatories and certificate holders (including natural persons, legal persons and other entities)\(^{14}\).
- The formalisation of common policy requirements, building on previous ETSI initiatives related to Signature Policies and RFC 3125\(^{15}\).
- Harmonised interface, access and input/output protocols to TSPs (including towards VSP and VAs). This should cover also TSPs-to-TSPs communications (e.g. VA-to-VA communication protocols).
- Continue work being done in the context of dissemination of trust status information with regards to determined services / products ancillary to electronic signatures (e.g. TSLs).
- X509 v3 certificate holder information extraction and semantic processing to ensure that the different certificate profiles can be mapped against a European Standard.

4.3.3 From a trust perspective

As was noted above, the supervision/accreditation approach already established by the eSignatures Directive is seen as an appropriate trust infrastructure that could be reused and extended into other TSP contexts. The establishment of the envisaged framework should thus build on:

- The Model of supervision / voluntary accreditation systems currently established for the CSPs issuing QCs and proposed to be extended to all types of TSPs. It is expected that such national systems could be extended to other TSPs than solely CSPs issuing QCs, but also that private or sector specific initiatives would result in certification or approval schemes on the basis of which the quality of TSP services could be assessed and the resulting approval status published.
- National Member States Trusted List and more generally on Trust Services Status Lists to disseminate approval status of TSP services in the context of determined approval status. This ensures that the supervision/accreditation approach has enough visibility and usability to actually benefit interoperability.

Commission Decision 2009/767/EC and ETSI TS 102 231 standard should both evolve consistently towards supporting the mutual recognition of approved TSP services.

A common basis for TSP services definition and quality criteria is of course of a crucial importance in this matter to ensure interoperability and cross-border use of such services, as was noted in the discussion of the required legal framework. Similarly, it is necessary that existing imperfections in the system are eliminated in as far as

---

\(^{12}\) Note that a proposal is to be finalised in the context of CROBIES study [RD3] and built upon various related models and initiatives including ETSI TS 101 456, 102 042, the PEPPOL approach, FBCA, NIST, OMB, Kantara, IDABC and other academic models.

\(^{13}\) This part is already addressed in CROBIES study (WP3).

\(^{14}\) CROBIES addressed the issue in the context of its proposal for harmonised qualified certificate profiles but more specifically this issue is addressed by the STORK large scale pilot. This issue may also encompass the mapping between signatory (certificate holder) identity profile towards other machine processable formats (e.g. XML).

\(^{15}\) Note that this is addressed by CROBIES in the context of its WP5.
possible, including though the definition of appropriate Conformity Assessment Guidance schemes to be applied in a consistent manner, and (where desired) the definition of common EU level accreditation schemes to ensure that accreditation can also have a beneficial impact on interoperability.

4.4 Stepwise and pragmatic roadmap towards a successful framework for interoperable and cross-border eSignatures

In the sections above, we already noted that we do not envisage a ‘big bang’ implementation of such a new framework, in which the existing legal/technical/trust framework would need to be entirely replaced in one single action. Rather, we envisage that the migration to such a model can be done through a gradual stepwise process, in which the existing framework is gradually tweaked, refined and expanded, until the situation as described above – a reworked and comprehensive framework for electronic signatures, including key ancillary services – has been established.

The following paragraphs propose a high level list of actions to be included in the context of the establishment of this vision, respectively on the legal, standardisation and trustworthiness tracks, followed by an proposed timeline for each of these tracks.

The hereafter listed action items do not have the aim to be either exhaustive or fully detailed; rather, they are intended to sketch the main action points to consider towards a reworked and comprehensive framework for electronic signatures and key ancillary services.

4.4.1 Legal track

The legal track would need to focus on establishing the legal framework mentioned above, consisting primarily of a revised Directive. This entails the following steps:

a) Defining the common section of the TSP Directive on a Community framework for electronic identification(ties), authentication, and signatures (IAS). This common part would act as a general framework applicable to any TSP service. Drafting, negotiating and establishing the following sections of this common part would be part of this action item:

i. Recitals and “whereas”
ii. Scope of the TSP Directive
iii. Definitions
iv. Fundamental concepts, principles and provisions applicable to all TSP services and service providers, including but potentially not limited to

a. technological neutrality,

b. legal equivalence (e.g. for qualified TSP services) / legal value rules (e.g. non deniable legal effect). This would relate to legal qualification and defined/standardised security/quality levels and associated criteria.

c. approach to standardisation (e.g. meeting generally recognised standards would provide legal presumption of compliance to ad-hoc legal provisions)

d. supervision and voluntary accreditation

e. market access
f. international market provision
g. liability principles
h. trustworthiness organised through trusted lists
i. data protection
v. International aspects (with efficient, pragmatic and sustainable mechanisms for ensuring international interoperability and mutual recognition)
vi. Committee and tasks of the Committee (if any)
vii. Notification (as related to the trustworthiness provisions)
viii. Review (with efficient, pragmatic and sustainable mechanisms to ensure efficient review)
ix. Implementation modalities

b) Specific sections of the TSP Directive. These sections should cover each type of trusted services in the IAS domain (e.g. CSPs issuing certificates, trusted time stamping/marking services, archiving services, signature policy issuance, identification services, authentication services, signature validation services, trusted services using electronic signatures like electronic registered mail services, etc.). Associated action items should include but not limited to the following:

i. Identification and definition of the trusted services and their associated component services;
ii. Identification and definition of the security / quality / policy levels and criteria associated to those services and the results (outputs) of those services;
iii. Specific legal concepts, principles and provisions applicable to each trusted service type (e.g. the above structure given for the common part can be used as draft skeleton), including legal qualification effect and value of related services outputs

The current eSignature Directive principles and provisions should constitute the starting point of the related specific sections. We do not envisage a big bang but a gradual stepwise migration towards a reworked and comprehensive framework for electronic signatures.

c) Specific principles for user and service provider devices should be addressed when relevant and further clarified.

d) Similar to a potential extension of Commission Decision 2003/511/EC mapping generally recognised standards to the current eSignature Directive, a new Decision (or several new Decisions) should be established to map generally recognised standards from the coming rationalised standardisation framework for electronic signatures as a result of mandate m460 [RD5]. This mapping, to be organised with a comprehensive perspective in mind (and not in a limited fashion as in current eSignature Directive) should allow market stakeholders to benefit from a legal presumption of compliance when generally recognised standards are met.

The completion of these action points and any other action items facilitating and supporting them should be achieved within the next 3-4 years according to specific priorities to be established by Member States on the basis of an iterative process ensuring:

1) Collection and analysis of existing MS national laws, especially with respect to ancillary services which are not comprehensively covered by the Directive;
2) An analysis of the ideal TSP Directive resulting in a draft proposal;
3) Collection and analysis of MS national inputs on the draft proposal (involving local legal experts, MS regulatory bodies, MS national supervisory, accreditation and (national) IT security bodies) as well as other key stakeholders (e.g. academics, industry, CIP Pilots, etc.);
4) Updated draft proposal for further evaluation and political consideration;
5) Final discussion and approval process.

4.4.2 Standardisation track

The main driver for the rationalisation of the European eSignature standardisation framework is the already existing Mandate m460 [RD5] with the specific inputs from the CROBIES study [RD3] supporting the EC Action Plan on e-identification and e-signatures [RD4].

The main objective of the mandate is to rationalise the existing standardisation framework around the various types of TSP services, the electronic signature creation and verification, as well as the secure user devices. The resulting European Electronic Signature Standards (EES) should be organised around three main cornerstones: the technical specifications (including policy requirements), the Conformity Assessment Guidance (on the basis of which supervision and accreditation system can be built), and the Implementation support (aiming to facilitate their use by stakeholders).

The scope and requirements from m/460 mandate and the already listed (see section 4.3.2) standardisation actions should be part of the 4 years work programme with some clearly identified “quick-win” tracks:

- Common definitions, specifications and policy requirements of the IAS & TSP products and services.
- Commonly defined identification elements (e.g. (sub)type identifiers) for those kinds of products and services components.
- The establishment of quality criteria for certificates and electronic signatures\(^{16}\), as well as for other Trust Service Tokens.
- The rationalised profile for Qualified Certificates\(^{17}\) and non-Qualified certificates.
- A common identification profile for signatories and certificate holders (including natural persons, legal persons and other entities)\(^{18}\).
- The formalisation of common policy requirements, building on previous ETSI initiatives related to Signature Policies and RFC 3125\(^{19}\).
- Harmonised interface, access and input/output protocols to TSPs (including towards VSP and VAs). This should cover also TSPs-to-TSPs communications (e.g. VA-to-VA communication protocols).

\(^{16}\) Note that a proposal is to be finalised in the context of CROBIES study [RD3] and built upon various related models and initiatives including ETSI TS 101 456, 102 042, the PEPPOL approach, FBCA, NIST, OMB, Kantara, IDABC and other academic models.

\(^{17}\) This part is already addressed in CROBIES study (WP3).

\(^{18}\) CROBIES addressed the issue in the context of its proposal for harmonised qualified certificate profiles but more specifically this issue is addressed by the STORK large scale pilot. This issue may also encompass the mapping between signatory (certificate holder) identity profile towards other machine processable formats (e.g. XML). CWA 16036 recommendations for unique identification systems for organisation and parts thereof should be considered and even extended to natural persons.

\(^{19}\) Note that this is addressed by CROBIES in the context of its WP5.
- X509 v3 certificate holder information extraction and semantic processing to ensure that the different certificate profiles can be mapped against a European Standard.
- A better coverage of all types of (secure) user devices.

The Conformity Assessment Guidance should be organised in such a way that they can serve as a complete basis for setting up national supervision/voluntary accreditation systems or market driven certification systems (e.g. CAG for certification services issuing certificates should be a complete alternative to US and commercial based systems like WebTrust for CA).

4.4.3 Trustworthiness track

This action plan track should be organised in such a way that one could leverage one of the most recent and significant step in the direction of trust in TSP services, namely the Trusted Lists as regulated in Commission Decision 2009/767/EC [RD6]. These trusted lists can already be used today under Commission Decision 2009/767/EC to list the supervision/accreditation status of any type of TSP services that would be supervised/accredited by Member States national bodies. Similarly market driven initiatives can use the same principles and underlying standards to further list approved services under a specific market driven approval scheme.

The establishment of a reworked and comprehensive framework for electronic signatures, including key ancillary services, relying on a common framework for legal, technical and policy requirements will be the necessary foundations of mutual recognition, interoperability and facilitation of use of electronic signatures, electronic identities and authentication services.
4.4.4 Proposed timeline

The graphical overview below shows a proposed consolidated visual roadmap for the establishment of this vision, with the main building blocks set out against an ideal but realistic timeline. This roadmap can be considered as a proposed Action Plan from the study team for the realisation of the vision described above.

![Diagram of Proposed Timeline]

**Figure 4**

The different stakeholders to be involved in implementing this vision vary from track to track and from building block to building block. Generally, the main stakeholders are expected to be the following:

- For the legal track: the main stakeholders will be the Member States and the Commission. Member States would benefit from informing the Commission of any local existing regulations for TSP services, which can serve as a best practice input for preparing an update of the European legal framework. On the basis of this, a new regulatory proposal can be drafted. Once adopted, it will be up to the Member States to implement the necessary framework at the national level. Both at the national level and at the European level, it will be crucial to ensure the transparency of this process, specifically by communicating with existing service providers that may be affected by the proposal, in order to avoid stagnation of market developments during the updating process.
For the standardisation track: interactions between the Commission and the relevant standardisation bodies play a central role, with the Commission's main role being to ensure that the standardisation bodies are aware of the broader perspective as described above during their work. Again, it will be important for this track to liaise with existing service providers, since the ongoing work can be expected to require implementation activities on their side.

For the trustworthiness track: the main stakeholders are the supervisory and accreditation bodies at the national or sectoral level, and the standardisation bodies who will be working on updating the relevant standards and guidelines (including with respect to trusted lists and the establishment of a common supervision/accreditation model). Implementation guidelines will also need to be made available to service providers to streamline and facilitate the supervision/accreditation process as far as possible.

It is clear from the overview above that a number of the building blocks required to realise the ideal framework are thus already being developed or examined in a number of different contexts, including the CROBIES initiative and the CIP pilots. A major challenge that was flagged by the CIP pilots (at least by representatives of the STORK and PEPPOL projects) is the long term sustainability of the results. In both cases, it was noted that the project results might be very promising for pilot purposes, but that their usage in practice in the long term required a consolidation process in which the outputs would be formalised, including through their integration into a generally applicable legal, technical and trust framework. The proposal above supports these needs, and would thus also support the long term sustainability of the pilot outcomes while integrating them into a more general and consolidated approach.