

Study on the standardisation aspects of eSignature

**A Study for the European Commission
(DG Information Society and Media)**

**By SEALED, DLA Piper
and Across communications**

EXECUTIVE SUMMARY OF THE FINAL REPORT

Date: 22/11/2007

Study on the standardisation aspects of eSignatures

Final Report

Published in November 2007

by

SEALED sprl
12 rue de la Paix, 7500 Tournai,
Belgium
RPM: BE 0876.866.142
www.sealed.be

Authors:

- Sylvie Lacroix (SEALED)
- Olivier Delos (SEALED)
- Patrick Van Eecke (DLA Piper)
- Michaël Custers (Across communications)
- Wim Janin (Across communications)

The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

1. INTRODUCTION

1.1 Context of the study

The present document is the Executive Summary of the Final Report of the *Study on the Standardisation Aspects of eSignatures* (INFSO 2006-0034).

The aim of the study is to provide the European Commission with the necessary information and assessment for a possible review of the standardisation needs in the field of electronic signatures supporting the European Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.¹

The Directive came into effect on 19 January 2000. Its purpose is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a harmonised legal framework for electronic signatures and for certain certification services in order to ensure the proper functioning of the internal market.

The business model of the eSignature directive is to have the market decide which technical solutions could be used for fulfilling the requirements of the directive, while ensuring legal compliance by referencing relevant standards in the Official Journal relating to some of the requirements of the annexes.

A set of electronic signatures standards has been developed by the European standardisation bodies CEN (European Committee for Standardisation) and ETSI (European Telecommunications Standards Institute) within EESSI (European Electronic Standardisation Initiative), on the basis of the requirements of the Directive.

Annex II(e) and Annex III of the Directive contain the requirements relating to the security of electronic signature products². According to Article 3(5) of the Directive, the Commission may establish and publish reference numbers of generally recognised standards for electronic signature products in the Official Journal of the European Communities.

Electronic signature products which comply with the generally recognised standards, the references of which have been published in the Official Journal of the European Communities, are presumed to be in conformity with the requirements of Annex II(e) and Annex III of the Directive. A list of generally recognised standards have been published in Commission Decision 2003/511/EC “on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the EP and the Council”³

1.2 Scope of the study

Article 2 of EC Decision 2003/511 states that the Commission shall review the operation of this Decision. This study was therefore called for to ensure that the technical requirements are fully analysed. The study analyses the use made by enterprises, market players and other stakeholders of the standards mentioned in this Decision and other related standards. The finding may help to assess

¹ OJ L 13, 19.1.2000, p.12.

² For the definition of “electronic signature product”, please refer to art.2§12 of the eSignature Directive

³ OJ L 175 15.7.2003, p.45.

whether the business model underpinning the eSignatures Directive is still relevant given the recent technological developments.

By assessing the model proposed by the Directive, the study aims to provide the information and assessment needed for a possible review of the needs for standardisation in this context and to design new standardisation tasks that will serve in future to establishing trust in e-transactions/e-services.

The **Study on the standardisation aspects of eSignature** has been conducted in three major phases whose results are summarised in the present executive summary of the final study report:

1. A **Field Survey** and analysis of the use of the standardisation work in operating eSignatures in the EU and EEA countries. This first phase covered the analysis of the existing EESSI standardisation work, the other relevant projects or standardisation initiatives supporting eSignatures, the already known eSignature applications and supporting existing or emerging technologies, as well as the related legal aspects linked to the Decision implementation in Member States and national related initiatives (e.g., interoperability). This analysis was supported by a field survey on the standardisation aspects of electronic signatures through an online survey and interviews of key stakeholders,
2. An **Assessment** of the adequacy of the eSignature standardisation model surrounding the 1999/93/EC Directive, and finally,
3. The **Recommendations** and **Conclusions** on the standardisation model and activities linked to the Directive.

2. SURVEY RESULTS

2.1 Survey respondents identification

With regards to the geographic locations of the respondents, the answers are quite well spread all over Europe and even beyond as from a representative total of 118 full entries, 101 answers are coming from 24 European countries, 5 answers from 3 EEA countries and 12 from other countries (including 5 from Turkey).

The interviewees are mostly coming from the application and service implementation side and in particular from the following categories:

- Application or Service Provider or supporting industry (36%),
- Certification Service Providers (CSP) or CSP supporting industry (22%),
- Public Authorities & Member States Policy makers (11%), and
- Opinion leaders from standardisation bodies (6%).

It is interesting to note that within these categories SME's are well represented (46%).

Very few end-user citizens have answered, not surprisingly, since end-users were not targeted as such but only the above stakeholders of the standardisation aspects of electronic signatures.

2.2 Context & Reasons for using Electronic Signatures

The very large majority of respondents are using (73%) or plan to use eSignatures (9%), and only a minority (18%) do not intend to use them.

Regarding the domains or types of eSignatures application, not surprisingly the large majority of respondents have indicated that they were using or that in their country **eGovernment** applications were used. The second most cited application domain (and closely to the eGov one) for electronic signatures current use is “**document signing**” whether PDF, Word, XML or emails. **eBanking/Finance**, internet banking, eInvoicing and eProcurement are respectively listed as used in decreasing occurrence. Some advanced services are also mentioned like archiving of signed documents. Mobile electronic signatures based on the standard series ETSI TS 102 203, 204, 206, and 207 have been implemented in two countries (TR, LT).

The large majority of the eSignature usages are intended for **open systems** as for closed systems the wide adoption and cost/efficiency interesting simple electronic signature implementations are more than sufficient and widely used. The types of implemented eSignatures are mostly Qualified (40%) or Advanced Electronic Signatures (38%), mainly supported by SSCD⁴ (60%) which is a (national) eID scheme in a lot of cases. Advanced ES are mainly supported by non-qualified certificates. In more than 50% of the cases, long term validity of the signatures needs to be ensured.

Regarding the technology that is used to support reported electronic signatures implementations, the most used (90%) is, surprisingly or not, based on Public Key Infrastructure (PKI). 88% of the interviewees use implementation with provided validation services (mostly CRLs and OCSP), generally with explicit validation policies. Long term validity of the signatures is offered in 55% of the cases and not provided in 32% of the implementation confirming a (s)low awareness of the crucial importance of such a service in the context of offering longstanding electronic signatures and the inherent flaw of PKI based technology in that matter without additional appropriate solutions.

About the expected promising technologies with regards to the (future) implementation of eSignatures, both mobile & wireless technologies and centralised signature-creating devices (for which the SSCD qualification or criteria for such a qualification is sought) are significantly emerging from the answers.

2.3 Context & Reasons for **not** using Electronic Signatures

For the online survey respondents that **are not using** eSignature, they do not do so primarily because they believe there is no real business need for it, secondly because it seems difficult to implement and thirdly because they believe the market not being mature enough.

2.4 Use of Electronic Signature Standards

Regarding the use of standards, it appears that the large majority (82,5%) of the respondents making use of eSignature are using standards. From this majority, 73% are using EU eSignature standards. Thus only 27% are using other standards and most often in addition to the EU standards, but rarely in place of EU standards. The reasons why people are using these standards are mainly because they help them to bring legal compliance to their applications, and secondly to meet their business needs.

⁴ SSCD stands for Secure Signature Creation Device as defined in the Directive 1999/93/EC (OJ L 13, 19.1.2000, p.12.)

Other standards used are mainly IETF PKIX RFC, ISO standards, X3C XMLSig and national standards (namely ISIS-MTT in Germany only, SEID in Norway and Sweden). The reasons why some people do not use the EU standards are mainly either because they do not perceive the benefit to follow them, or because another framework was available or simply as a result of a lack of awareness.

2.5 Opinions on eSignature Standards Complexity

Most of the respondents using EU standards already have a certain expertise with these EU Standards. However, the opinion of the interviewees on the **standards** clearly shows that they find the standards:

- **Rather or too complex**
- **Too numerous** (with still even some identified gaps)
- While the level of coherence and completeness satisfies the majority of the interviewees, **lack of explanation on the coherence between the standards**
- **Are difficult to find**
- Related documentation regarding **guidelines and implementation samples are not sufficient** or not good enough.

Regarding these aspects of the EU eSignature standards, we can highlight the following requirements from the opinions expressed by the interviewees:

- **Business and practice based standards are wanted:** The current standards are considered as suffering from the following drawbacks
 - o Too many possible implementation options reducing the chance for practical interoperability;
 - o Too many possible interpretations
 - o Too academic and not enough business practice oriented
 - o Not enough high level straight-talking description to help newcomers in eSignature implementation
 - o Not self explanatory
 - o No implementation samples
 - o Not enough commercially available standards compliant software
 - o Lack of clear link with the laws
- **An international dimension is required** (outside EU)
- **True standards** are wanted rather than standardisation deliverables without a clear and formal status
- **One single easy to access and to understand repository** for eSignature related standards

The area covered by electronic signature standards is complex by nature. Currently, PKI technology is the sole technology able to meet the requirements from Advanced electronic signatures and thus of qualified electronic signatures. Although it is a mature technology, which is being more and more implemented, even in very large scales implementations, it remains a rather complex technology that now becomes intertwined with legal requirement. Consequently, the combination of technical and legal requirements makes it difficult for both technical and legal experts to implement a legally compliant electronic signature technology.

A wide framework and set of standardisation deliverables for electronic signature products (CWA-CEN Workshop Agreement⁵ and ETSI TS-ETSI technical specification) have been developed on the

⁵ CEN Workshop Agreements (CWAs) are CEN publications. They are consensus-based specifications, drawn up in an open Workshop environment. Note that the legal value of CWA is not yet clearly defined as they are not assigned the status of a

basis of the requirements of the Annexes to Directive 1999/93/EC to support implementation of eSignatures. Unfortunately, the current standardisation model of the Directive is only partially supporting this framework: indeed, the 2003/511/EC Commission Decision only lists some generally recognised standards of which conformity with the requirements of Annex II(f) and Annex III of the Directive is presumed. The very short list of published standards in the 2003/511/EC Commission Decision is exclusively related to:

- (i) the usage of electronic signature products and (Hardware) Security Module by a CSP issuing digital certificates and
- (ii) the Secure Signature Creation Device criteria.

Adequation of published recognised standards vs market needs

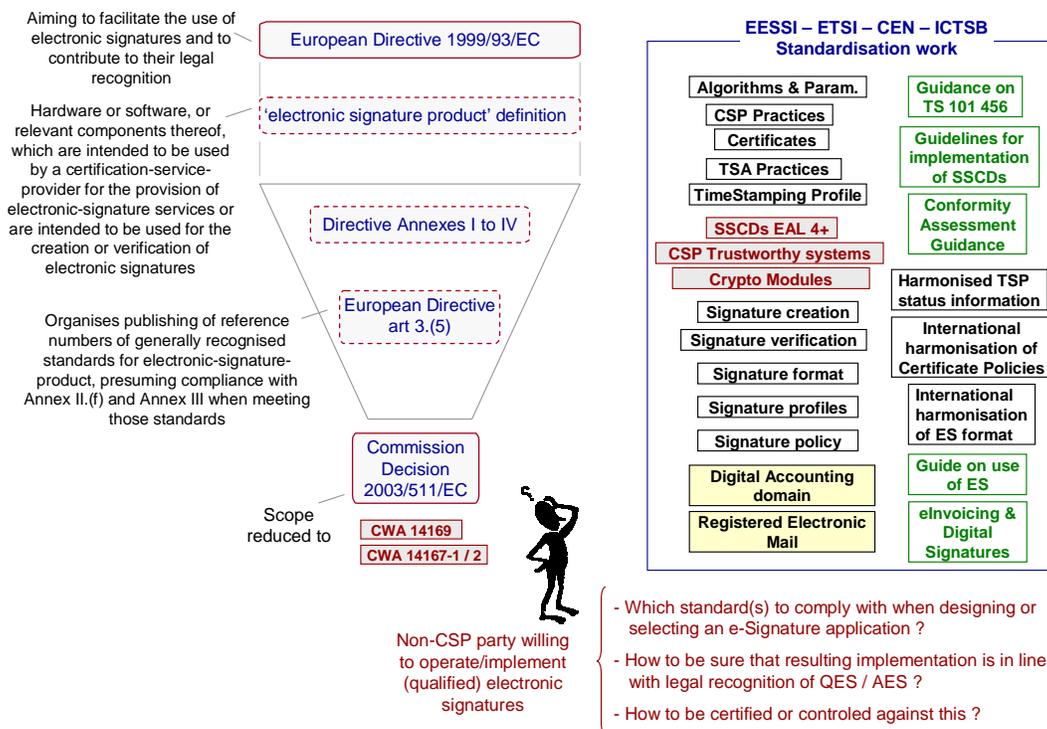


Figure 1

As illustrated in the above Figure 1, this limited publication reduces considerably the scope of the standardisation deliverables officially referenced to support the Directive. Indeed the purpose of the 1999/93/EC Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. The “electronic signature product” definition in Art. 2.2 of the Directive, and as being the subject of its Article 3.5 is however not restricted to its usage by the CSP issuing certificates. It also covers the electronic signature products or applications as developed by an Application/Service Provider and used by a signatory and/or verifier to create and or verify electronic signatures (whatever the appropriate CSP selected by the user to issue (qualified) certificates to support the user’s electronic signatures). Additionally it also covers other types of Certification Service Providers providing

formal standard (EN), are not designed to support legislative requirements while the concept of CWAs does not in itself precludes this possibility. Further discussion on the legal assessment of the CWAs can be found in the final report.

electronic signatures services than the sole CSPs issuing certificates. This includes but is not limited to Timestamping service providers, (Long Term) Archiving services, etc. (Directive 1999/93/EC, Article 2.12 and recital (9)).

Considering this, based on discussions with stakeholders from diverse sides of electronic signature operations⁶, and as confirmed by the general perception coming out of the online survey performed in the context of the study, it clearly appears that, while nearly (but not) all aspects of operating electronic signatures have been standardised or normalised, there is a huge lack of a more high level overview, guidelines, criteria, standard or whatever formal document against which any Application/Service Provider could refer to in order to have a full confidence that its electronic signature application or implementation:

1. is meeting the Directive requirements when desired,
2. is reaching legal recognition,
3. is likely to be as interoperable as possible with other similar schemes, and
4. can be used for cross-border business transactions when needed.

2.6 Usefulness of EU eSignature Standards

More encouraging are the results concerning the perceived **usefulness** of the standards:

- 74% of the respondents affirm that the standards help them to comply with laws.
- A little more than 60% of the respondents claim standards are at least slightly helpful to meet their business needs.

2.7 Market expectations on EU eSignature Standards

Regarding the ideal eSignature standardisation approach, a majority of the interviewees are seeking:

- a formal way of working,
- encompassing a list of standards and guidelines to follow, and
- possibly accompanied by an official certification.

Their expectations from the standards themselves are clearly to reach:

- a maximum level of **interoperability** (within and beyond Europe),
- the **legal recognition** of eSignatures for which a better link with standards is required and a better link between standards themselves, and
- easy implementations through a clear set of guidelines.

⁶ Stakeholders, either from the CSP side, or from the Application/Service Provider side developing electronic signature products or services, or from the Time Stamping Service Provider side, or when advising customers on correctly implementing and operating (qualified) electronic signatures.

2.8 Marketing aspects

Slow market activity in (qualified) electronic signatures

From the huge majority of the interviewees, the perceived reasons for the slow market activity in (qualified) electronic signatures are the complexity of the technology in general and in particular the complexity of related standards that are not based on business practices. This results in high market prices and costly implementations for which there is no perceived business benefit compared to the existing solutions. As a result, too few applications have been made available. The lack of promotion and awareness of the electronic signature solutions is next cited as an important reason.

However, respondents from DE, CZ and IT experience a very big growing trend in the number of applications as pushed by law, eGovernment initiatives and even service oriented business models.

The emergence of national eID schemes is another key factor that indicates a take-off of processes dematerialisation within which eSignatures are key building blocks.

Marketing and Promotion of the eSignature standards

Regarding the marketing of the eSignatures standards, the efforts of the European Commission are considered as insufficient. The interviewees are mainly expecting the Commission to perform active promotion and marketing efforts around those eSignature standards. Efforts are also expected from the Commission with regards to clear guidelines on the way of dealing with standards in order to implement (legally) recognised signatures.

2.9 Opinion from European Standardisation Organisation interviewees

The main message from the stakeholders involved in the standardisation processes, whether they are member of a European Standardisation Organisation (ESO) or involved experts in the drafting of standards or ESO deliverables, is that the “standardisation process” is not understood or even known to the target users of these documents. The drafting of standards is always the compromise between the academic quality of the documents and the interests of the drafting process initiators (who are looking first on their return on investment and competitive advantage).

The majority of the standardisation actors stress the fact that the standardisation process must be more driven by the business not meaning the sole technology providing industry but the real business actors of each specific application domain. Forum initiatives, like electronic signature aspects in eInvoicing, grouping business, legal and technical experts should be further exploited for all other business domains.

The cost/benefit aspects must also be taken into consideration when drafting standardisation in these matters.

The recognition of electronic signature standards will come from the business. That is why the standardisation work must be driven by the real business requirements, clearly mapped to the legal requirements in order to ensure the legal compliance when this is possible. Standards should give the appropriate technical and economical implementation guidance in order to have good quality implementation (not highest quality but appropriate quality with regards to cost/benefit and appropriate risk mitigation in the covered business domain) with a maximised level of interoperability.

Less options and more straight-talking and practice oriented guidance⁷ will also be the key to practical interoperability.

2.10 The question of QES versus other levels of ES

The question can be asked whether one should focus so much on qualified signatures (sometimes difficult to develop because of many requirements and hence more expensive; the QES level is not always necessary; the use of it for legal purposes is overestimated, etc.). Why not just accept that qualified signatures are a bridge too far?

The answer is that although qualified signatures are not always necessary to implement, it helps interoperability and risk management because qualified signature technology is well standardised and documented. It is furthermore legally rewarding as it is equivalent to handwritten signatures for which a clear and non-ambiguous case law exists.

The study has clearly identified that the existence of QES is seen as an incentive for the deployment of e-signature thanks to the clear definition of QES (what is it “technically”, what are the related policies and practices for CSP issuing qualified certificates and expected to comply with this appellation and what is the expected legal value). This precise definition helps people to feel at ease on “what to do” and sustains interoperability.

However, this level of signature requires a quite costly implementation. Many organisations would like to opt for a lower level of signature, knowing that the legal effect of those cannot be denied. Unfortunately, technically speaking, there are numerous ways of implementing AES and this refrains the use of AES because interoperability is difficult to achieve (what are the equivalence and levels of AES?). In front of a judge, the most “well implemented” solutions will get more chance to be agreed. It is wish able to have something to rely on helping the judge to assess the level of AES and/or helping the signatory / relying party to argue on tangible elements. There is a CWA (14365-1/2) that aims to classify different levels of AES. It is a “descriptive text”, but as a CWA, what is the value of such a non formal document. In addition, this CWA is not marketed and lastly, too vague and not up-to-date (and even rather incorrect). It is suggested that the content of this CWA needs to be revised, to be externalised and officialised in some way.

On the other hand more and more Member States will implement a citizen electronic identity card that is likely to support qualified electronic signatures. Currently 71 QCAs are available in 15 European countries and others are in preparation phase. Those QCAs and qualified national eID schemes are making QES affordable and are key factors of eGov and business processes dematerialisation.

2.11 Conclusions

There is a clear requirement to better derive the eSignature standardisation deliverables and standards from real business needs and business practices. The Directive business and standardisation models should consider and reference those standardisation deliverables that will support the real market and business needs and expectations within the applicable legal constraints or in other words solving the following equation:

$$\text{Business needs} + \text{legal framework(s)} = \text{supporting technical specifications (standards)}$$

⁷ Such guidance should not turn into an increase of constraints that would impede the interoperability objective by blocking/slowing the developments.

The eSignature related standardisation framework should not only be better in line with business practices but should also be accompanied by a single and easy to access document providing **explanation and coherence between existing and future standardisation deliverables**. This can even be organised on specific themes whether in terms of electronic signature products or per business or application domain.

In order to further assist eSignature stakeholders in their implementation and use, **straight-talking implementation profiles, guidelines and samples** should be made available for real and practical business contexts.

Regarding the expected strength and value of the eSignature standardisation deliverables, **true standards** with an **international dimension** are wanted rather than standardisation deliverables without a clear and formal status.

The marketing aspects of the eSignature standardisation model and deliverables are certainly not the least aspects that should be taken into consideration. Active promotional and marketing efforts are expected from the Commission. They should be organised around, or at least include, the realization of a **single, easy to access and to understand repository** gathering the eSignature related standards and the supporting information.

3. ASSESSMENT – WAS THE BUSINESS MODEL RIGHT?

One can question the success of the business model adopted by the policy makers, i.e. linking the publication of some standards to a legal presumption of conformity with some legal requirements. Was the business model the right model?

3.1 *Successful model for what has been published as generally recognised standard*

When considering the standardisation deliverables referenced by the Decision 2003/511/EC, one can say that, yes, the business model has finally succeeded. It has even succeeded as well as for those other standardisation deliverables that have been further developed around them and included by reference (either normative or informative) in these Decision 2003/511/EC referenced CWAs.

The Decision 2003/511/EC specifically focused on only one part of the elements covered by the “electronic signature product” definition (Directive 1999/93/EC, Article 2.11⁸). It indeed only covers those product elements related to the Certification Service Provider issuing (qualified) certificates (with reference of Article 3.5 presumed compliance with Annex II.f) and Secure Signature Creation Devices (with reference of Article 3.5 presumed compliance with Annex III).

In that specific context of CSP certification activities, delivering and/or supported by SSCDs, one can say that after having experienced strong difficulties⁹, this market is now indeed becoming quite mature, stabilised and even flourishing in some countries like Italy, Spain or Germany. At the time of the study, it can be seen that 15 countries in the EU have at least one Qualified CA for a total of 71 QCAs issuing qualified certificates¹⁰. The main driver for this new age for the already 30-year old PKI technology and in particular for the Qualified CAs is the national electronic identities established and deployed by more and more Member States. eGov is in the driving seat for the deployment of PKI based QCAs as well as for the top listed applications as demonstrated by the online survey.

Most of these Qualified CAs, when not all, are using or are at least compliant with the published recognised standards (i.e., CWA 14167 1-2, CWA 14169) and even those informatively or normatively referenced in those published standards (such as ETSI TS 101 456, ETSI TS 101 862, ETSI 102 176-1/2, see final report for more details). This is mainly because the Member States’ administration in charge of supervising and/or accrediting their national Qualified CAs have harmonised their supervision and accreditation criteria on those CEN and ETSI standards, notably through their participation to the Article 9 Committee and through the Forum of European Supervisory Authorities for Electronic Signatures (FESA).

⁸ Directive 1999/93/EC, Article 2.12: ‘electronic-signature product’ means 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.

⁹ Some CSPs have stopped their activities or were in real business difficulties at the early stages in absence of real market like in Denmark or in Austria.

¹⁰ Additional countries are currently on the way of experiencing the set-up of Qualified Certification Authorities, in particular in the context of national eID schemes but not exclusively (e.g., PT, LU, MT). It has also been reported that some countries (like France) do not have QCAs because of the unlimited liability to be endorsed by a QCA. It would be however clearly wrong to say that this is a requirement from the Directive. When such an unlimited liability requirement is imposed on QCAs, this may be due to national rules regarding liability (for services provided to the public).

3.2 *Not fully successful model*

It can be observed that although the standardisation deliverables (CWAs) that have been referenced in the O.J. have been well implemented by the market, the other deliverables have not all experienced the same level of success. We identified the following reasons and related issues that have lead to this unbalanced market uptake and which are still hindering the full uptake of electronic signatures in the internal market:

- **Incompletely implemented business model:**
 - The **lack of transparency** with regard to the current standardisation deliverables (their legal value, their internal connection and their connection with the directive, and with other existing standardisation international framework) and the different legal approaches towards these deliverables have created a lot of confusion in the market. This is mainly due to the hybrid business model of the Directive (it is not a New Approach Directive but it uses New Approach methods).
 - Directive’s **lack of definition or requirements related to the whole set of “electronic signature products”**. Besides signature creation or verification products, some CSP services (like the intrinsically required time stamping and archiving services, but also emerging electronic signatures related services like registered electronic mail, etc.) are neither fully nor clearly covered by the Directive, are using the standards when available but also more formal and international standard framework.
 - The **referencing issue**, that is the lack of referenced standards outside the standards related to Annex II (f) and Annex III. The other standardisation documents produced within EESSI and following are not referenced.
 - The **lack of formal standards** in the area of electronic signatures. The standardisation deliverables developed within EESSI are not formal standards in the sense of ENs. The referenced documents are only CWAs and the non-referenced ESO deliverables are CWAs, ETSI TS or TR. Their value is different from real EN documents; they are often not regarded as real standards by the market.
- **Business issues related to the electronic signature standards**
 - They are not business practice standards as no formal and representative business requirement collection and analysis are performed or taken into account when drafting them.
 - They are not formal standards and as not referenced, their value is questioned. They are not regarded by the Business as real standard in the sense of they have neither a legal value (for those not referenced) nor full standard value as they are only “deliverables” from ESOs.
 - They are not subject to any formal public enquiry or voting process before publication as they are only ESO deliverables and not formal standards.
 - They are too complex because of intrinsic complexity of matter, but also because of drafting rules procedures enabling ESO member to draft deliverables for their own interests as competitive advantage, lack of global view on the set of standards, lack of guidelines and implementation samples, etc.

- They are not self explanatory and no global overview with a single repository presenting them in a coherent and consistent way (e.g., in function of the types of electronic-signature-products).
- There is no (or not enough) clear link with the Directive’s requirements (when any).
- **Interpretation of Directive and ESO deliverables is not managed globally** but separately from legal, business and technical point of view
- **Lack of marketing and promotional efforts** of existing electronic signature standards

Thus,

- the system of referencing a few standards, and by referencing giving them more legal value (i.e. presumption of conformity),
- producing other standards within CEN/ETSI but not referencing them, and thus not giving them more legal value
- limiting the standardisation work to CWAs and not EN, i.e. not real standards

has caused lots of confusion in the market.

In other words, the system of referencing works well (when applied), and it is a pity that it was limited to annex II (f) and III.

3.3 The referencing issue

Lack of referenced standards outside annex II (f) and annex III (or broader the lack of formal support of the existing standards by the Commission) was the result of the strict interpretation of Article 3.5, sentence 2 which exclusively refers to the referencing of standards relating to Annex II (f) and III as to their legal compliance. Other standards have consequently not been referenced.

We however do believe that the Commission can do more than it is doing now to reference standards outside Annex II (f) and Annex III, although it is not possible to ensure legal compliance solely by referencing them because of the limitation in phrase 2 of Article 3.5 of the Directive, unless the Directive is changed. The legal basis of our belief is to be found in the Directive itself in its Article 3.5, sentence 1.

Publishing other references in the Official Journal through a decision while clearly stating that legal compliance is not presumed (unless another solution could be found to confer either a legal compliance with the applicable requirements) would be a pragmatic and practical solution to confer a strong moral recognition to the work that has been done and is still done by the ESOs in the context of electronic signatures.

The legal basis allowing the EC to publish reference numbers of the other electronic signature standards in the OJ can be found in the directive itself:

Article 3.5, phrase 1: *“The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities”.*

We are of the opinion that this first phrase can be read without linking it to the second phrase. The publication of the reference numbers is however limited to electronic-signature products.

An “electronic-signature product” is defined by the directive as “*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.*” This definition is however wide enough to cover all market needs when implementing electronic signatures. And in any case, an electronic signature product is broader than CSP trustworthy systems (Annex II (f)) and secure signature creation devices (Annex III). The referencing (or mapping) between the types of electronic signature products that should be fully covered by the Directive and the existing or future electronic signature standards can be, according to the above definition, illustrated in the below Figure regarding the current Decision 2003/511/EC and the recommended new (updated) Decision.

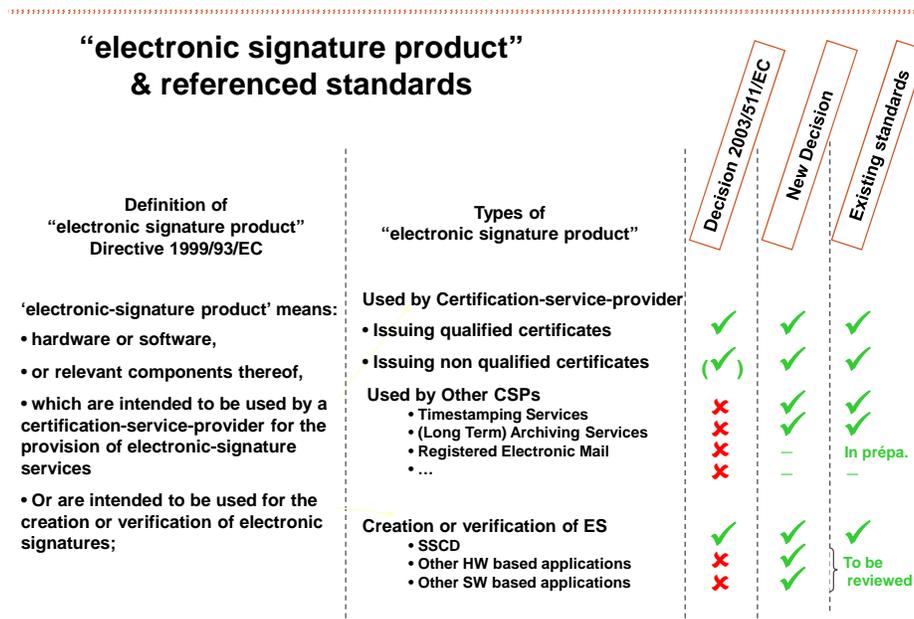


Figure 2: Electronic signature product coverage by Decision 2003/511/EC and by standardisation efforts

Conclusion on the referencing issue:

- Without changing the directive, it is not possible to publish references to generally recognised standards in the OJ **ensuring legal compliance**, other than standards relating to Annex II (f) and Annex III.
- Without changing the directive, it seems possible to publish in the OJ references to generally recognised standards relating to all types of electronic signature products¹¹, but without ensuring legal compliance for those not relating to Annex II(f) or Annex III. Legal basis for this publication is in our opinion article 3.5, sentence 1.
- Without changing the directive, it seems possible to publish in the OJ references to standards (not necessary “generally recognised”) related to Signature Verification Devices (SVD) in order to include and cover all aspects of this type of electronic signature products. Legal basis

¹¹ For the definition of “electronic signature product”, please refer to art.2§12 of the eSignature Directive as illustrated in Figure 2.

for this publication is in our opinion article 3.6 while it is true that SVDs are already part of electronic signature products and can thus be covered by 3.5, sentence 1.

3.4 *The business needs issue*

The business needs issue is more related to the fact that Business requirements are not correctly collected and analysed when drafting electronic signature ESO deliverables and resulting in:

- Not business practice standards
- Too complex or not even feasible
- No real standard
- No evaluation / voting process before publication of standards (ESO deliverables)
- Not self-explanatory (both individually and as a whole set of standards)
- Unclear link with the Directive requirements when any

There is a clear need for more involvement and considerations of business representatives in the drafting of electronic signature standards, and a re-design (or repositioning) of the existing standards versus this “business practice standard” objective and even initiate new standardisation tasks to meet this same objective and fill the potential gaps.

As already stated before, the recognition of the European electronic signature standards will come from the business. That is why the standardisation work must be driven by the real business requirements, clearly mapped to the legal requirements in order to ensure the legal compliance when this is possible, and standards should give the appropriate technical and economical implementation guidance in order to have good quality implementation (not highest quality but appropriate quality with regards to cost/benefit and appropriate risk mitigation in the covered business domain) with a maximised level of interoperability. Less options and more guidance will also be the key to practical interoperability.

4. RECOMMENDATIONS

4.1 Legal and policy related recommendations

No directive review - Opening the directive for review would allow the EU institutions to adapt some rules to the current reality. The legal compliance presumption of article 3.5 could, for example, be broadened to other requirements than Annex II (f) and Annex III. Also, specific internal market rules could be incorporated for other certification services (e.g. archival services, time stamping services). We do however not recommend opening the directive for review because of its cumbersome and time consuming procedures. It is clearly possible to significantly improve the Directive business model and its success without changing the Directive. Furthermore, opening the directive for review may re-open lengthy discussions between the Member States on the issue of authentication and electronic signatures. Considering the fact that since end 1999, the market has taken a few years to know it, use it and rely on it to build products, changing the Directive may also introduce perturbation due to the changes and time to reassess the products.

New Commission Decision – The current Commission Decision 2003/511/EC is out of date and limited to the publication of references to standards in compliance with Annex II (f) and Annex III of the directive. We therefore recommend drafting a new Commission decision:

- Amending or repealing Commission Decision 2003/511/EC
- Updating the list of generally recognised standards ensuring compliance with Annex II (f) and Annex III
- Adding a list of generally recognised standards for electronic signature products (but explicitly stating that legal compliance is not presumed as per art.3.5¹²) covering all types of electronic signature products, i.e. those hardware, software or component thereof to be used:
 - o By a Certification Service Provider (CSP) for the issuing of qualified certificates
 - o By a CSP for the issuing of provision non qualified certificates
 - o By a CSP for the provision of other electronic signature services, including but not limited to Time-stamping services, (Long Term) Archiving services (in particular when related to signed data and associated electronic signatures), Registered Electronic Mail, etc.
 - o For the creation or the verification of electronic signatures.
- This includes adding a list of (generally recognised) standards for signature verification devices in the light of the recommendations for secure signature verification laid down in annex IV and in the interests of the consumer (but explicitly stating that legal compliance is not presumed).
- Adding a list of generally recognised standards relating to advanced electronic signatures originating in third countries (but again, explicitly stating that legal compliance is not presumed).

¹² However the referencing of these standardisation deliverables would provide them with the recognition that is expected by the market.

4.2 Standardisation related recommendations

We also recommend the European Commission to issue a mandate to the European Standardisation Organisations (CEN/CENELEC/ETSI) asking them to draft a guidance paper on the use of the standards, including their legal relevance. This document should be as practical as possible and point stakeholders (developers, users, ...) to the differences between the standards. The document could be in the form of a list of existing standards, describing their internal relationship, their legal value and their compliance presumption or not with the directive. The document must be initiated in the light of the “Business Practices Driven – Legal framework governance – Technical Expertise Support” philosophy in order to maximise meeting the expressed business requirements. This document must be written in parallel and take into account an in-depth review and assessment of every existing standard under the light of this same “towards business practice standards” philosophy. It is likely that it will be mainly the ESOs deliverables related to the “electronic signature products to be used for signature creation and verification” that will require the major changes.

In order to respond to the problem that current electronic signature standards are too academic and do not come from real business needs, we recommend the European Commission to bring together the industry (builders and users of electronic signatures solutions), standardisation experts (ESOs), technical experts, policy experts in a platform within a structure ensuring a clear leadership and guidance with regard to roadmap of the review of existing electronic signatures standardisation deliverables and the future standardisation works on electronic signatures.

We also recommend the European Commission to undertake the necessary efforts for promoting to ENs the CWAs and ETSI TSs or TRs that will be included in the New Decision. Since this is not the task of the Commission but of the European Standardisation Organisations, the Commission cannot do more than informing these organisations about its desire.

Also, we recommend the Commission to adopt a policy for ICT standardisation: the EU legislator has so far developed no particular model comparable to the New Approach in the internal market laying down the rules, conditions and criteria for developing standards in the framework of other policy areas, including the ICT. In the Commission’s Staff Working Document *The challenges for European standardisation*, the idea of having standards supporting EU policies in the ICT area but without embedding this role into a specific legal framework has been put forward¹³. A 2007 study commissioned by DG Enterprise on the specific policy needs for ICT standardisation has identified a number of issues that could arguably challenge the current system of EU ICT standardisation policy. The study also proposes a model for developing an EU ICT standardisation policy capable of responding to the challenges imposed by the changing ICT and ICT standardisation landscape.¹⁴

4.3 Quick-wins on Qualified CA recognition and QES validation

Considering the unclear publication of the results of the implementation of Article 11 of the eSignature Directive regarding the supervised or accredited “Qualified” quality of a Certification Authority, and in order to facilitate the validation of a Qualified Electronic Signature, several quick-win actions are recommended to the European Commission:

¹³ Commission Staff Working Document, *The challenges for European standardisation*, p. 16. On 18 October 2004, the Commission adopted a Communication on “the Role of European Standardisation in the Framework of European Policies and Legislation” accompanied by a staff working paper dealing with “The challenges for European Standardisation”. Both documents analyse the current situation of European standardisation and identify the key areas where the European standardisation system and the instruments available to European standardisation policy can and should be further improved.

¹⁴ See DLA Piper, Uninova, Technical University of Delft, “EU Study on the specific policy needs for ICT standardisation”, July 2007, 148 pages. (www.ictstandardisation.eu).

- Collect the name and addresses of all accredited (art.11 §1.c) **and** non accredited but supervised Qualified CAs from all Member States and EEA countries;
- For each technical QCA¹⁵ from these supervised or accredited legal entities, collect the following information:
 - o Issuing CA identifying information (e.g., Common Name CN, Organisation O, Country C)
 - o Certificate Policy identifier (CPS) and repository location (an English version should be at least available)
 - o Presence of the ETSI TS 101 456 QCP+ certificate policy identifier in the end-user qualified certificates (QCP+ to ensure that the qualified certificate has been issued on an SSCD and that it is guaranteed by the issuing QCA)
 - o Presence of the QCStatement extension in the end-user qualified certificates

Note that the above information may not be harmonised and implemented by all QCAs in Europe. The collection of this information will allow assessing such a fact. It would be recommended to enforce the implementation of a harmonised set of minimal information within qualified certificates as part of the supervision and accreditation rules in order to allow harmonised and straightforward validation of a qualified certificate.

- Officially publish and maintain the list of all supervised and accredited QCAs with the above collected information per QCA

From a pure technical point of view and from the content of the supporting certificate, it can be verified that an electronic signature is indeed a qualified electronic signature¹⁶ but this is only a claimed assertion that should be verified from a trusted authority or source that indeed the issuing CA is a supervised or accredited QCA according to the eSignature Directive and its implementation in the Member States from which the QCA is originating. However as further detailed in annex B of the study final report no such trusted source is currently available making it difficult to verify such claimed assertions.

Additional measures may be taken to ensure the practical validation of qualified electronic signatures with regards to the automation of verification of the qualified status of an issuing CA, or with regards to the various forms of electronic signature formats (in particular XAdES and CADES).

4.4 Marketing related recommendations

We furthermore recommend the European Commission to undertake the necessary marketing efforts for promoting the use of the European electronic signature standards:

- within the EU in order to dynamize the full uptake of electronic signatures in the internal market, and
- outside of the EU (based on article 7.2), “in order to facilitate the legal recognition of advanced electronic signatures originating in third countries”.

¹⁵ Or group of technical QCAs when several are used to issue identical qualified certificate profiles (e.g., there are so far at least 54 Belgian technical QCAs issuing the millions of Belgian qualified certificates for the national eID cards.

¹⁶ At least until the suspension or revocation of the supporting certificate unless appropriate trusted time assertion has been associated to the electronic signature.

4.5 Implementation of the recommendations – organisational model

As we have seen before, the eSignature Directive business model consisting in copying the system of new approach to a certain extent for a non new approach matter, linking the publication of some standards to a legal presumption of conformity with some legal requirements, is not wrong by essence and it has reasonably well functioned for those standardisation deliverables that have been referenced. On the other hand success is not there for the rest of the mass of standardisation deliverables that has been produced to cover the electronic signature areas not covered by the 2003/511/EC referencing decision.

In order to further and even drastically improve the efficiency of this business model, and by then better meet the objective of the eSignature Directive to facilitate the use of the electronic signature and its legal recognition, there is no fundamental need to change the Directive or the basic principle of its business model. The solution is to fully implement this business model while considering and referencing those standardisation deliverables that will support the real market and business needs and expectations within the applicable legal constraints or in other words solving the following equation:

$$\text{Business needs} + \text{legal framework(s)} = \text{supporting technical specifications (standards)}$$

Without changing the directive, and based on its article 3.5, it seems possible to publish in the OJ references to generally recognised standards relating to all types of electronic signature products, but without ensuring legal compliance for those not relating to Annex II(f) or Annex III.

It is recommended to organise this global reshaping and reviewing of eSignature standardisation through the set-up of a “European Electronic Signature Forum” or “Committee” whose working philosophy should be the above mentioned equation, as illustrated in below Figure 3.

Global re-shaping & reviewing of eSignature standards

Business drive (requirements) → within legal framework(s) → supported by technical specifications (standards)

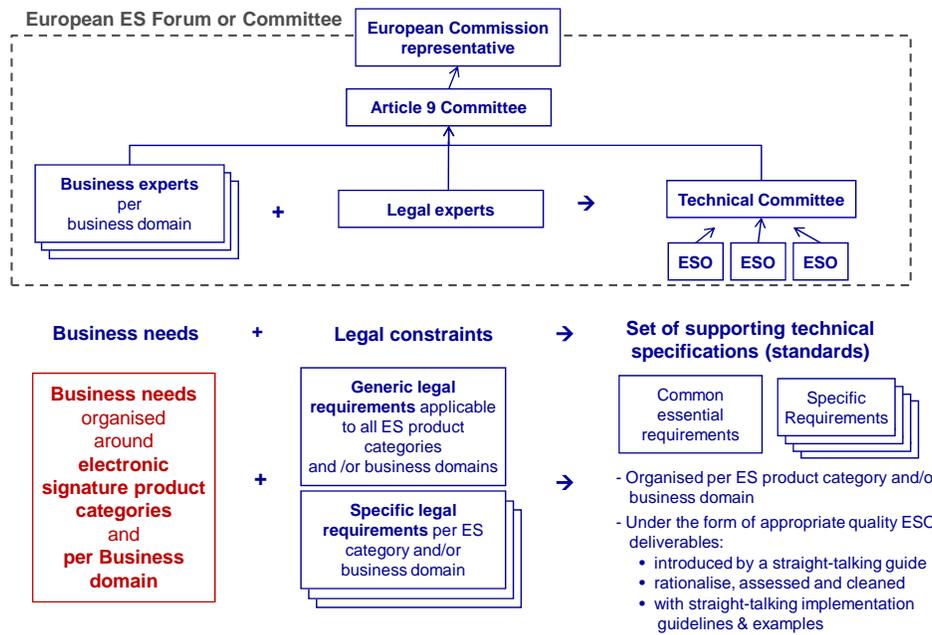


Figure 3: European Electronic Signature Forum or Committee

The objective of this Forum or Committee would be to re-organise, rationalise and potentially correct or complete the existing eSignature standardisation deliverables to efficiently support the real business needs in their legal constraints. These first tasks should be included within a roadmap that will also consider future ES related standardisation tasks and/or existing deliverables evolution in order to cope with state-of-the-art of technologies and future business needs.

The work of this Forum or Committee should be driven by the Business Needs organised around the electronic signature product categories and per business domain¹⁷. Business experts coming from the various considered business domain should be represented in the Forum or Committee as the main driving force.

Those Business Needs should be placed into their respective global and specific legal constraints when related to the implementation of electronic signatures. To support this, legal experts should be integrated into the Forum or Committee.

Considering those business needs within their legal constraints, the set of supporting/applicable standardisation deliverables should then be organised and defined¹⁸ through the involvement of technical experts in close collaboration with the ESOs. These standardisation deliverables should be organised per electronic signature product category and per business domain gathering common essential requirements and specific requirements as further illustrated by Figure 4.

Each set of so organised and business practice oriented standardisation deliverables should:

- Be introduced by a practical guidance on the use of the related deliverables (this could be considered as the main deliverable to be referenced in the context of a determined ES product category, as all other would be normatively included by reference),
- Be business practice rationalised, assessed and cleaned from the existing deliverables,
- Be accompanied by a set of straight-talking implementation guidelines and code samples,
- Receive a formal “standard” status (at least for the referenced deliverables, but this may not be the case for those deliverables included by reference in published standards).

It is important to note that per “electronic signature product” category, the set of standards (blue box in the right part of Figure 4) should be less numerous as possible while covering all related aspects. They should be “covered” by a *guidance* deliverable (that could be the referenced main (standard) deliverable providing clear chart and explanation about the consistency between them to support the related business application domain (left part of Figure 4) within the applicable legal framework (middle part of Figure 4). It is also important to ensure that requirements that are essential to an electronic signature product category are commonly reflected whatever the business application domain while authorising specific requirements with regard to the considered business application domain (kaki boxes).

¹⁷ “Business” in the widest and global sense and not restricted to the restricted ESO definition or members.

¹⁸ Mostly from the existing set of standardisation deliverables as illustrated in Figure 3, while better organising them, correcting those that must be corrected, and filling potential gaps, and rationalising their number.

Global re-shaping & reviewing of eSignature standards

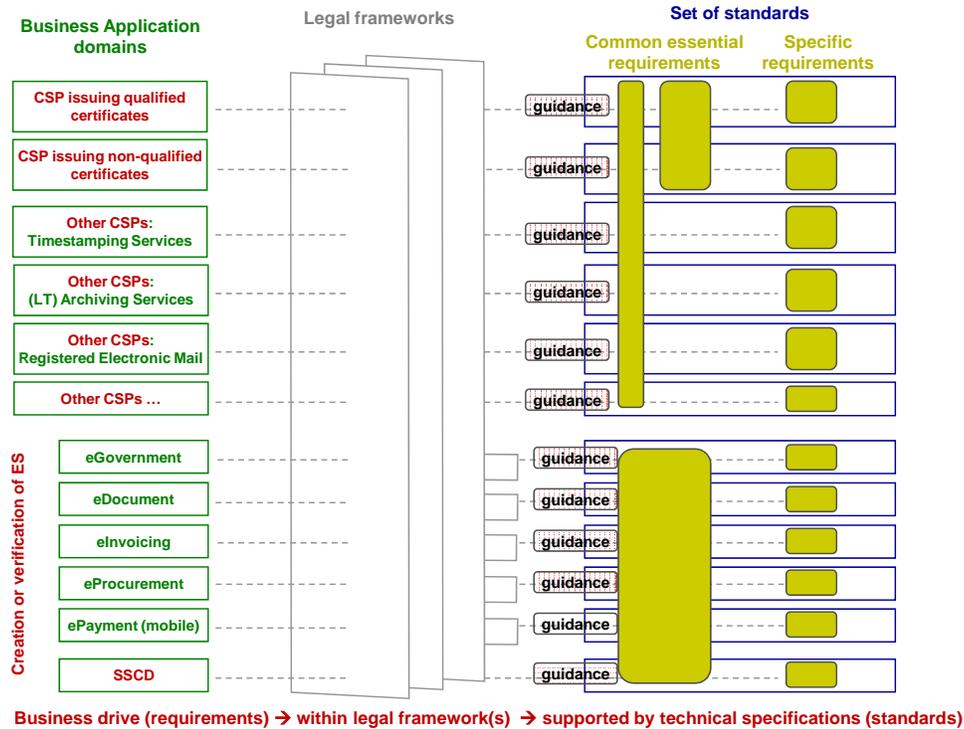


Figure 4: Restructuring the eSignature standardisation deliverables per ES product categories

For the sake of comparison, the existing eSignatures standardisation deliverables as presented in Figure 1 can be grouped per ES product category as presented in below Figure 5, with the following legend:

- in white, the current deliverables related to the CSP issuing qualified and non qualified certificates and to the SSCDs;
- in red stripes, the current deliverables related to the CSP providing other electronic signature services, such as timestamping service providers, and registered electronic mail;
- in solid red, the current deliverables related to the creation and verification of electronic signatures.

In addition to the reshaping of the current eSignature standardisation deliverables in accordance with the previously described requirements, including the associated guidance(s) on those deliverables, it is also strongly recommended that a clear and straight-talking map (or chart) of all eSignature deliverables will be made publicly available (even better organised than the one presented in Figure 5) and be used to give easy access to all related deliverables. Appropriate marketing and awareness efforts should be performed by the Commission.

Acronyms

AdES	Advanced Electronic Signature
CA	Certification Authority
CAdES	CMS (Cryptographic Message Syntax) Advanced Electronic Signature
CEN	Centre Européen de Normalisation
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Services Provider
CWA	CEN Workshop Agreement
EESSI	European Electronic Signature Standardisation Initiative
EN	European Norm
ES	Electronic Signatures
ETS	European Technical Specifications
ETSI	European Telecommunications Standards Institute
EU	European Union
HS	Harmonised Standard
IE	Internet Explorer
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
MS	Member State
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
QES	Qualified Electronic Signature
RFC	Request For Comment
S/MIME	Secure Multipurpose Internet Mail Extensions
(S)SCD	(Secure) Signature Creation Device
SVD	Signature Verification Device
TR	Technical Report
TS	Technical Specification
TSA	Time-Stamping Authority
TSP	Time-Stamping Policy
URL	Uniform Resource Locator
XAdES	XML Advanced Electronic Signatures (enhances XMLDSig)
XML	Extensible Markup Language
XMLDSig	XML Signature