ETSI draft SR 000 000 V0.0.2 (2011-08)

Special Report

Rationalised Framework for Electronic Signature Standardisation

Reference
DSR/ESI-000099

Keywords
e-commerce, electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
© Comité Européen de Normalisation Electrotechnique 2011.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Contents 3
Intellectual Property Rights 4
Foreword 4
Introduction 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definitions, abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 8
4 Inventory 9
5 Rationalised Structure for Electronic Signature Standardisation Documents 10
5.1 Introduction 10
5.1.1 Objectives of the rationalised framework 10
5.1.2 Approach 10
5.2 Electronic Signature Standardisation Classification Scheme 11
5.2.1 Functional Areas 11
5.2.2 Document Types 13
5.2.3 Rationalised Framework with Sub-Areas 14
5.2.4 Numbering Scheme 15
5.3 Rationalised Framework by Area 16
5.3.1 Generic 16
5.3.2 Signature Creation & Validation 16
5.3.3 Signature Creation Devices 23
5.3.4 Cryptographic Suites 25
5.3.5 TSPs Supporting Electronic Signatures 26
5.3.6 Trust Application Service Providers 29
5.3.7 Trust Service Status Lists Providers 32
6 Gap Analysis 34
7 Work Plan 34
Annex A: Discussion on TSP and CSP Concept 35
Annex B: Initial Guidance on Matching Business Requirements to Electronic Signature Standards from Signature Creation / Validation Viewpoint 36
B.1 Introduction 36
B.2 The Guidance Approach 36
B.3 Business factors 36
Annex C: Inventory 41
History 42

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Special Report (SR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI) and CEN Technical Committee TC 224.

Introduction

As a response to the adoption of Directive 1999/93/EC [i.1] on a Community framework for electronic signatures in 1999, and in order to facilitate the use and the interoperability of eSignature based solution, the European Electronic Signature Standardization Initiative (EESSI) was set up to coordinate the European standardization organisations CEN and ETSI in developing a number of standards for eSignature products.

Commission Decision 2003/511/EC [i.2], on generally recognised standards for electronic signature products, was adopted by the Commission following the results of the EESSI. This decision fostered the use of eSignature by publishing "generally recognised standards" for electronic signature products in compliance with article 3(5) of the Directive but has a limited impact on the mapping of the current state of the European standardisation on eSignatures, which also covers ancillary services to eSignature, and the legal provisions and requirements laid down in Directive 1999/93/EC.

Emerging cross-border use of eSignatures and the increasing use of several market instruments (e.g. Services Directive [i.3], Public Procurement [i.4], eInvoicing [i.5]) that rely in their functioning on eSignatures and the framework set by the Signature Directive emphasized problems with the mutual recognition and cross-border interoperability of eSignature.

Intending to address the legal, technical and standardisation related causes of these problems, the Commission launched a study on the standardisation aspects of eSignature [i.6] which concluded that the current multiplicity of standardization deliverables together with the lack of usage guidelines, the difficulty of access and lack of business orientation is detrimental to the interoperability of eSignature, and formulated a number of recommendations to mitigate this. Also due to the fact that many of the documents have yet to be progressed to full European Norms (ENs), their status may be considered to be uncertain. The Commission also launched the CROBIES study [i.7] to investigate solutions addressing some specific issues regarding profiles of secure signature creation devices, supervision practices as well as common formats for trusted lists, qualified certificates and signatures.

In line with Standardisation Mandate 460 [i.8], consequently issued by the Commission to CEN, CENELEC and ETSI for updating the existing eSignature standardisation deliverables, the current document establishes a rationalised framework to overcome these issues within the context of the Signature Directive, taking into account possible revisions to this Directive, and proposes a future work programme to address any elements identified as missing in this rationalise framework.

1 Scope

The present document establishes a rationalised framework for electronic signature (eSignature) standardisation within the context of the current Electronic Signatures Directive and its possible revision. It provides:

a) A rationalised structure for future European eSignatures standardisation documents.

b) An inventory of existing electronic signature standardisation.

c) The results of a gap analysis with an assessment of the existing eSignatures standardisation documents.

d) The proposed future work plan for filling the gaps in electronic signature standardisation identified through the analysis.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.2] Commission Decision 2003/511/EC of 14.7.2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.

[i.3] Directive 1998/34/EC of the European Parliament and the Council of 22.6.1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.

[i.4] Directive 2004/18/EC of the European Parliament and Council of 31.3.04 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts and Directive 2004/17/EC of the European Parliament and Council of 31.3.04 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors.

[i.5] Council Directive 2006/112/EC of 28.11.06 on the common system of value added tax.

[i.6] "Study on the standardisation aspects of e-signatures", SEALED, DLA Piper et al, 2007.

NOTE: Available at http://ec.europa.eu/information_society/policy/esignature/docs/standardisation/report_esign_standard.pdf

[i.7] "CROBIES: Study onCross-Border Interoperability of eSignatures", Siemens, SEALED and TimeLex, 2010.

NOTE: Available at http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm

[i.8] 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".

[i.9] EFVS Study Framework contract ENTR/05/58-SECURITY, SC N°14: " Final Report on Common Solution Model: Completion of the framework for Signature Validation Services", February 2010.

NOTE: Available at http://ec.europa.eu/idabc/servlets/Docf934.pdf?id=32633.

[i.10] ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.11] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

[i.12] W3C Recommendation: "XML Signature Syntax and Processing (Second Edition)", 10 June 2008.

[i.13] ISO 32000-1: "Document management -- Portable document format -- Part 1: PDF 1.7".

[i.14] Commission Decision 2011/130/EU of 25 February 2011 establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.15] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.16] IETF RFC 3161 (August 2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol".

[i.17] CCMB-2006-09-001: "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1", September 2006.

[i.18] ITU-T Recommendation X.509 | ISO/IEC 9594-8 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

[i.19] Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

[i.20] Commission Decision 2010/425/EU of 28 July 2010 amending Decision 2009/767/EC as regards the establishment, maintenance and publication of trusted lists of certification service providers supervised/accredited by Member States.

[i.21] ITU-T Recommendation X.eaa | ISO/IEC 3rd CD 29115 -- Information technology – Security techniques – Entity authentication assurance framework.

3 Definitions, abbreviations

3.1 Definitions

The following terms and definitions are taken from Directive 1999/93/EC [i.1]:

advanced electronic signature: electronic signature which meets the following requirements:

a) it is uniquely linked to the signatory;

b) it is capable of identifying the signatory;

c) it is created using means that the signatory can maintain under his sole control; and

d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

certificate: electronic attestation which links signature verification data to an entity or a legal or natural person and confirms the identity of that entity or legal or natural person

certification service provider: entity or legal or natural person who issues certificates or provides other services related to electronic signatures

NOTE: See Annex A for discussion on certification service providers and Trust Service Providers. In the present document we will use the term "Trust Service Provider issuing certificate" for designating the Trust Service Provider who issues certificates and provides related certificate creation, assignment and life cycle management services.

electronic signature (eSignature): data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication

qualified certificate: certificate which meets the requirements laid down in Annex I of Directive 1999/93/EC **[i.1]** and is provided by a certification service provider who fulfils the requirements laid down in Annex II of Directive 1999/93/EC **[i.1]**.

qualified electronic signature: advanced electronic signature which is based on a qualified certificate and which is created by a secure signature creation device.

Note: See article 5.1 of Directive 1999/93/EC [i.1].

signatory: 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: Directive 1999/93/EC [i.1] defines a signatory as being a "person", which "person" can be interpreted as a natural person or a legal person when this is applicable in MS legislation

signature creation data: unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature

signature creation device: configured software or hardware used to implement the signature-creation data

secure signature creation device: signature creation device which meets the requirements laid down in Annex III of Directive 1999/93/EC [i.1].

signature verification data: data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature

signature verification device: configured software or hardware used to implement the signature-verification data.

For the purposes of the present document, the following terms and definitions also apply:

Information Preservation Service Provider (IPSP): Trust Application Service Provider which provides Trust Services to which information, among which documents, is entrusted in an agreed form (digital or analogue) for being securely kept in digital form for a period of time specified in the applicable agreement; this service is expected to be able to exhibit all preserved information at any moment during, or at the end of, the preservation period

registered e-mail: enhanced form of mail transmitted by electronic means (e-mail) which provides evidence relating to the handling of an e-mail including proof of submission and delivery

registered electronic delivery: enhanced form of electronic delivery which provides evidence of relating to the handling of electronic messages including proof of submission and delivery

registered electronic delivery service provider: trust application service provider which provides registered electronic delivery trust services

registered e-mail service provider: trust application service provider which provides registered e-mail trust services.

signature generation service provider: trust service provider which provides trust services that allow secure remote management of signatory's signature creation device and generation of electronic signatures by means of such a remotely managed device

signature policy: set of rules for the creation and validation of Electronic Signatures that defines the technical and procedural requirements for creation, validation and long term management of an Electronic Signature, in order to meet a particular business need, and under which the signature(s) can be determined to be technically valid

NOTE: It has been identified that this term "Signature policy" has created confusion in the market as it both applies to a document covering extended business model involving one or more signatures and describing rules on a business level and on the other side technical formats of machine processable information limited to the processing of one single signature. The future work of the STF will be to further analysis this aspect in the gap analysis and recommend future work.

signature validation service provider: trust service provider offering services in relation validation of Electronic Signatures.

NOTE: Based on the definition given in [i.19].

TEMPORARY NOTE: It has been identified that this term and concept deserves more work in the current standardisation framework and will be dealt in the context of the gap analysis and recommendation for future work.

time-stamping service provider: trust service provider which issues time-stamp tokens

NOTE: This entity may also be referred to as a Time-Stamping Authority.

time-stamp token: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time

trust application service provider: trust service provider operating a value added Trust Service based on Electronic Signatures that satisfies a business requirement that relies on the generation/verification of Electronic Signatures in its daily routine

NOTE: This covers namely services like registered electronic mail and other type of e-delivery services, as well as long term storage services related to signed data and Electronic Signatures.

trust service: electronic service which enhances trust and confidence in electronic transactions.

NOTE: Such Trust Services are typically but not necessarily using cryptographic techniques or involving confidential material.

trust service provider: entity which provides one or more electronic Trust Services.

NOTE: See Annex A for discussion on certification service provider and Trust Service Provider.

trust service status list: signed list presentation of the Trust Service status information on which interested parties may determine whether a Trust Service is or was operating under the approval of any recognized scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place

trust service status list provider: trust service provider issuing a Trust Service Status List

trust service token: physical or binary (logical) object generated or issued as a result of the use of a Trust Service

NOTE: Examples of binary Trust Service Tokens are certificates, CRLs, Time-Stamp Tokens, OCSP responses, evidence of delivery issued by a REM Service Provider.

trusted list: national supervision/accreditation status list of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC

NOTE: Based on definition given in [i.19].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AdES	Advanced Electronic Signature
$AdES_{QC}$	Advanced Electronic Signature supported by a Qualified Certificate
API	Application Program Interface
ASiC	Associated Signature Containers
CA	Certification Authority
CABForum	CA Browser Forum
CAdES	CMS Advanced Electronic Signature
CEN	Comité Européen de Normalization
CRL	Certificate Revocation List
CSP	Certification Service Provider
EN	European Norm
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IAS	Identification, Authentication and Digital Signature
IPSP	Information Preservation Service Provider
LoA	Level of Assurance

NOTE: As specified in [i.21].

OCSP	Online Certificate Status Protocol
PAdES	PDF Advanced Electronic Signature
PKC	Public Key Certificate
QC	Qualified Certificate
QES	Qualified Electronic Signature
RED	Registered Electronic Delivery
REM	Registered Electronic Mail
SGSP	Signature Generation Service Provider
SP	Signature Policy
SR	Special Report
SSCD	Secure Signature Creation Device
SVSP	Signature Validation Service Provider
TASP	Trust Application Service Provider
TR	Technical Report
TS	Technical Specification
TSL	Trust-service Status List
TSP	Trust Service Provider
TSP_{PKC}	Trust Service Provider issuing Public Key Certificates
TSP_{QC}	Trust Service Provider issuing Qualified Certificates
TSSLP	Trust Service Status List Provider
TSSP	Time-Stamping Service Provider
XAdES	XML Advanced Electronic Signature
XMLDSig	XML Digital Signature

NOTE: As specified in [i.12].

4 Inventory

As a major input to the development of the rationalised framework an inventory has been collected of existing standardisation and publicly available specifications. This ensures that the rationalised framework has a sound basis of all the known specifications and provides a reference point for the gap analysis.

This inventory includes standards, publicly available and regulatory specifications from the International, pan European, national and sector (e.g. banking, e-invoicing, biopharmaceutical) domains.

The information has been collected from information known to the specialist task force developing this framework and provided by stakeholders.

The detailed data collected in the inventory is provided in Annex C.

TEMPORARY NOTE 1: It is recognised that for the public review draft this information is incomplete. Any party aware of information relevant to the inventory is requested to provide input through the email address provided for comments on this framework.

TEMPORARY NOTE 2: Annex C is provided as a separate document in the public review draft of this document.

A copy of the inventory in Excel spreadsheet form is available as a separate download through the ETSI / CEN Electronic Signature Standards web site.

5 Rationalised Structure for Electronic Signature Standardisation Documents

5.1 Introduction

5.1.1 Objectives of the rationalised framework

The objectives of the rationalisation of the structure and presentation of the European Electronic Signature standardisation documents are:

- To allow business stakeholders to more easily implement and use products and services based on electronic signatures. A radical business driven and guidance approach will underlie the rationalisation exercise of the eSignature standardisation framework. Business driven guidance will be provided for maximising successful implementation of eSignatures based products, services and applications by guiding the stakeholders through the definition and parameterisation of the different elements or components of eSignatures and/or eSignature based services/applications and guiding them consequently through the selection of the appropriate standards and their implementation.
- To facilitate mutual recognition and cross-border interoperability of eSignatures.
- To simplify standards, reduce unnecessary options and avoid diverging interpretations of the standards.
- To target a clear status of European Norm for standardisation deliverables whenever this is applicable.
- To facilitate a global presentation of the eSignature standardisation landscape, the availability and access to the standards.

5.1.2 Approach

The central stone of such a rationalisation exercise will indeed naturally be the creation and validation of electronic signatures. Of course, as business stakeholders even not familiar with eSignature underlying technology may already have deduced from Directive 1999/93/EC on a Community framework for eSignatures, the creation and validation of electronic signatures cannot be achieved in a fully opened environment without relying on one or several third party services, tools or products. This namely covers digital certificate issuers to attest the identities of signatories, time-stamping provider to attest trusted time association to a signature or an event, signature creation device issuers, and many other services related to the creation, validation and/or preservation of electronic signatures. Such third parties moreover need to be trusted to some extent for providing their services in accordance with the expected legal or technical specifications. For this, one may rely on specific approval schemes operated by trustworthy organisations.

For those target audiences being stakeholders willing to introduce and implement eSignatures in a business electronic process, the rationalised framework will provide a reading angle focusing on the creation/validation of eSignatures. This will aim to guide them on how to implement eSignatures in a business electronic process to support business risk or security risk mitigation when setting-up an e-process from scratch or moving from a paper-based process to an e-process. It will also focus on positioning creation/validation of eSignatures against the output of the provision of services supporting such creation/verification and potentially the preservation of such signatures. This viewpoint will provide both guidance on defining and configuring the different eSignatures components as being relevant in the related business context and the selection of the appropriate standards and their implementation.

For those target audiences being business or governmental entities willing to set-up and operate trusted services either supporting the creation/verification of electronic signatures or building up added value Trust Services relying on the generation/verification of eSignatures for its daily routine, the rationalised framework will provide an appropriate focusing on the provision of such services while relying on the different relevant elements of the framework.

Specific care will be taken during this rationalisation exercise, not only in its definition phase but certainly in its implementation phase on the simplification of the standards by reducing unnecessary options, avoiding diverging interpretations, by better mapping them to business driven practices and legal provisions and in particular to reaching cross-border interoperability.

In order to facilitate (cross-border) mutual recognition of eSignature based solutions, services and products, this framework shall also aim to provide a rationalised and common basis for approval schemes through the definition of standard requirements for the assessment of such solutions, services and products against the electronic signature standards to ensure conformant solutions at common levels of security.

In addition, through the provision of a common basis for interoperability and technical conformity testing specifications and facilities, the framework assists in assuring that these solutions can be both conformant to specifications and interoperable.

5.2 Electronic Signature Standardisation Classification Scheme

In order to meet its objectives and in particular simplification requirements for the standardisation landscape and its structuring, as well as requirements on the accessibility to the relevant standards and their presentation, the rationalised framework has been organised around 6 (functional) areas and 5 types of documentation.

5.2.1 Functional Areas

The 6 areas for standardisation of eSignatures are the following:

1) **Signature Creation and Validation:** This area focuses on standards related to the creation and validation of electronic signatures, covering:

   i. the expression of rules and procedures to be followed at creation, verification and for preservation of eSignatures for long term,

   ii. signature format, packaging of signatures and signed documents,

   iii. and protection profiles for signature creation/verification applications.

2) **Signature Creation Device**: This area will focus on standards related to Secure Signature Creation Device as defined in the Signature Directive, on signature creation devices used by Trust Service Providers as well as other types of signature creation devices.

3) **Cryptographic Suites**: This area covers standardisation aspects related to the use of signature cryptographic suites, i.e. the suite of eSignature related algorithms including key generation algorithm, signing algorithms with parameters and padding method, verification algorithms, and hash functions.

4) **Trust Service Providers supporting eSignatures:** This includes TSPs issuing qualified certificates, TSPs issuing public key certificates other than qualified certificates, Time-Stamping Services Providers, TSPs offering signature validation services, TSPs offering remote signature creation services (also called signing server). The current list covers those services supporting electronic signature which exist to date; other Trust Services may be identified at a future date.

NOTE: Trust Service Providers supporting eSignatures is closely related to Certification Service Provider as defined in the Electronic Signature Directive [i.1]. See Annex A for a discussion on the concept of TSP and CSP.

5) **Trust Application Service Providers:** This covers Trust Service Providers offering value added services applying electronic signatures and that relies on the generation/verification of electronic signatures in normal operation. This includes namely registered mail and other e-delivery services, as well as long term archiving services. This list may be extended as further services applying electronic signatures are identified.

6) **Trust Service Status (List) Provider**: This area covers the standardisation related to the provision of trust service status lists.

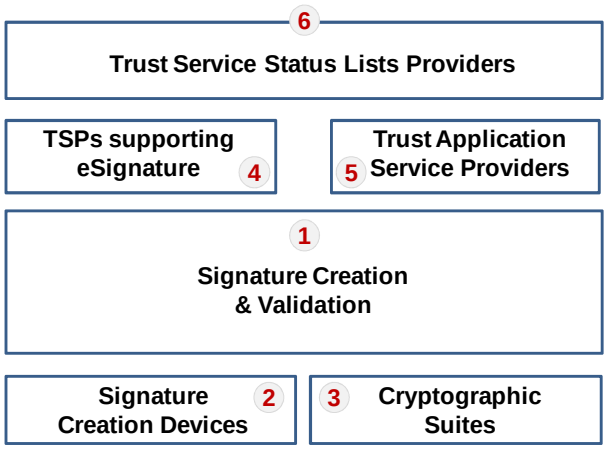


Figure 1: Overview of the Rationalised Framework for electronic signature standardisation

Depending on the target audiences, different viewpoints can be used for approaching the rationalised framework for electronic signature standardisation. Guidance documents (see Annex B) will guide the stakeholder on how to implement the relevant entry point standards and to position them against the other standardisation areas, the selection of the appropriate standards and their implementation as illustrated in the following Figures.

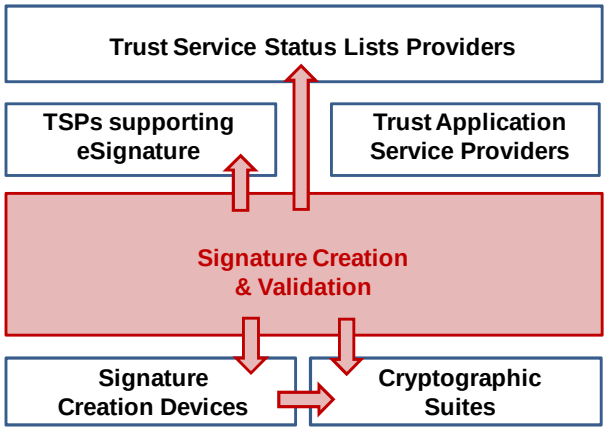


Figure 2: Signature Creation & validation viewpoint of Rationalised Framework

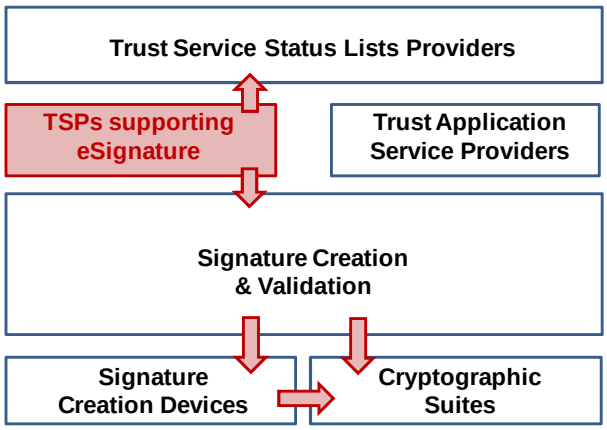


Figure 3: TSPs supporting eSignatures viewpoint of Rationalised Framework

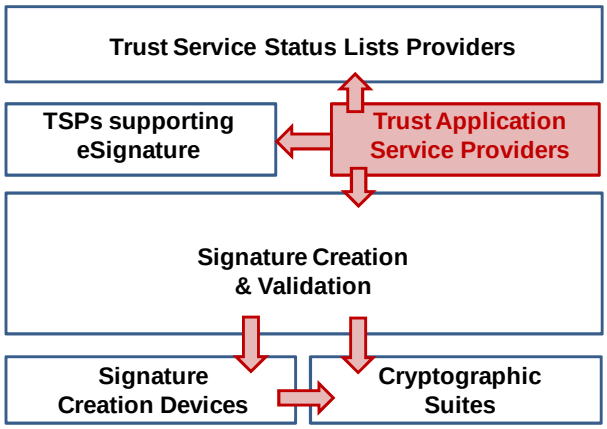


Figure 4: Trust Application Service Providers viewpoint of Rationalised Framework

5.2.2 Document Types

The documents required for standardisation of each of the above electronic signature functional areas have been organised around the following five types of documents:

1) **Guidance:** This type of documents does not include any normative requirements but provide business driven guidance on addressing the eSignature (functional) area, on the selection of applicable standards and their options for a particular business implementation context and associated business requirements, on the implementation of a standard (or a series of standards), on the assessment of a business implementation against a standard (or a series of standards), etc (see Annex B on initial thoughts on guidance).

2) **Policy & Security Requirements:** This type of document specifies policy and security requirements for services and systems, including protection profiles. This brings together use of other technical standards and the security, physical, procedural and personnel requirements for systems implementing those technical standards.

3) **Technical Specifications:** This type of document specifies technical requirements on systems. This includes but is not restricted to technical architectures (describing standardised elements for a system and their interrelationships), formats, protocols, algorithms, APIs, profiles of specific standards, protection profiles, etc.

4) **Conformance Assessment:** This type of document addresses requirements for assessing the conformance of a system claiming conformance to a specific set of technical specifications, policy or security requirements (including protection profiles when applicable). This primarily includes conformance assessment rules (e.g. common criteria evaluation of products or assessment of systems and services).

5) **Testing Compliance & Interoperability:** This type of document addresses requirements and specifications for setting-up interoperability tests or testing systems or for setting-up test or testing systems that will provide automated checks compliance of products, services or systems with specific set(s) of technical specifications.

Figure 5: Illustration of Document Types in the Rationalised Framework

5.2.3 Rationalised Framework with Sub-Areas

This rationalisation of the structure for eSignature standardisation framework for some area can be broken down into further sub-area as illustrated in Figure 6 below. This identifies the primary sub-areas within the six eSignature (functional) areas as described here above. For each area, a common set of 5 types of document will address aspects applicable to all sub-areas, and per sub-area additional documents address aspects specific to each sub-area.

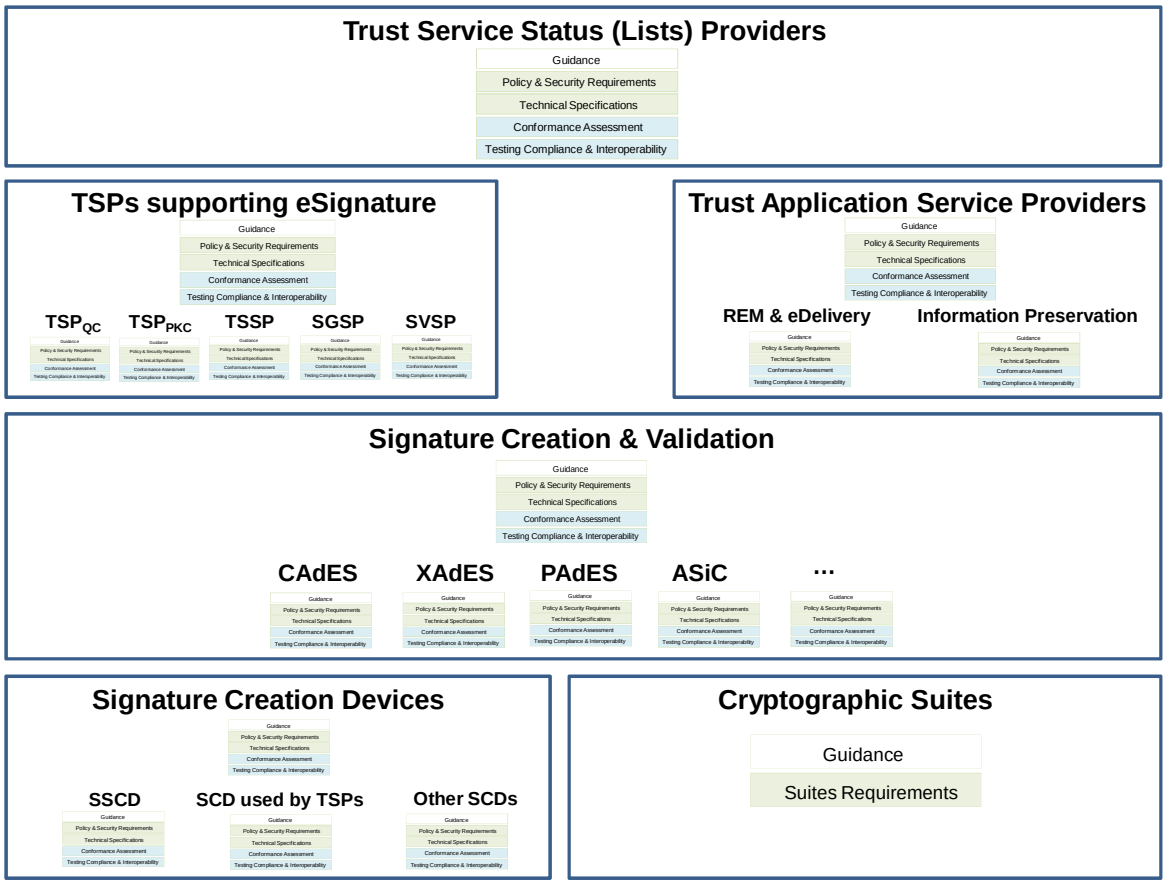
So far sub-areas have been identified in areas 1, 2, 4, and 5.

In the Signature Creation and Validation area 1, we have identified sub-areas focusing on the specific standardised Advanced Electronic Signature formats, respectively CAdES, XAdES and PAdES, as well as the Advanced Signature Container format of containers that bind together a number of signed data objects with Advanced Electronic Signatures applied to them or time-stamp tokens computed on them.

In area 2, Signature Creation Devices, three sub-areas have been identified to group documents with regards to the type of signature creation device, namely Secure Signature Creation Devices (SSCDs), signature creation devices used by Trust Services Providers (TSPs) and other signature creation devices.

Area 4, TSPs supporting eSignatures, has been divided in sub-areas focusing on the different types of such TSPs, namely Trust Service Providers issuing Qualified Certificates (TSP_{QC}), Trust Service Providers issuing public key certificates which are not qualified (TSP_{PKC}), Time-Stamping Service Providers (TSSPs), Signature Generation Service Providers (SGSPs) and Signature Validation Service Providers (SVSPs).

Area 5, Trust Application Service Providers, contains two sub-areas, respectively the one dedicated to Registered Electronic Mail (REM) and Registered Electronic Delivery (RED) services provisioning, and the one dedicated to Information Preservation Service Providers (IPSP).



 © ETSI 2011. All rights reserved

Figure 6: Illustration of Rationalised Framework with Sub-areas

5.2.4 Numbering Scheme

A **consistent numbering** for such documentation will be searched with the aim to identify a single and consistent series of eSignature standards (e.g. the 66 000 series) and with the aim to enable each document to keep the same number whatever maturity level it reaches through its lifetime. The current numbering scheme that is likely to be exploitable is defined as follows:

DD L66 xxx-z-w Vm.a.b

Where:

DD indicates the deliverable type in the standardisation process (SR, TS, TR, and EN)

L identifies type deliverable in the standardisation process:

0 for Special Reports (SR)

1 for Technical Specification (TS) and Technical Report (TR)

3 for European Norm (EN)

NOTE 1: This numbering is in line with ETSI practices. The level 2 are used for ETSI specific types not relevant to the current document.

66 indicates the series of standardisation documents related to eSignatures

NOTE 2: This will be replaced with the number assigned to this series of standards.

xxx indicates the serial number (000 to 999)

where **X**xx identifies the area (0-generic to a number of areas; 1-signature creation and validation; 2-signature creation devices; 3-cryptographic suites; 4-Trust Service Providers supporting eSignatures; 5-Trust Application Service Providers; 6-Trust Service Status (Lists) Providers)

where x**X**x identifies a sub-area within the identified area, or 0 for documents generic to a given area

where xx**X** identifies the type of document (0-Guidance; 1-Policy and Security Requirements; 2-Technical Specifications; 3-Conformance Assessment; 4- Testing Compliance and Interoperability))

-z-w identify respectively multi-parts and sub-parts of those multi-parts as some documents may be multi-part documents, or even multi-part documents with sub-parts.

Vm major version number

a technical version number

b editorial version number

5.3 Rationalised Framework by Area

5.3.1 Generic

The generic document for electronic signatures includes:

TR 166 000 Rationalised Framework for Electronic Signature Standardisation

This document is to provide the framework for the 66 000 series of documents on Electronic Signature standardisation. It will be based on the contents of the present document. It will specify the schema for electronic signature standardisation. It will also provide the basis for the provision of business guidance provided in the other areas and reference the business guidance for signature creation and verification (TR 166 100) as the recommended starting point for the analysis of requirements in particular for those target audiences being stakeholders wishing to introduce and implement eSignatures in a business electronic process.

5.3.2 Signature Creation & Validation

The documents for electronic signature standardisation for signature creation and validation are summarised in table 1 with further details provided below:

Table 1: Standards for Signature Creation and Validation

			Signature Creation and Validation			
			Sub-areas			
						Guidance
TR	1	66	1	0	0	Business Driven Guidance for Signature Creation and Validation
						Policy & Security Requirements
EN	3	66	1	0	1	Policy & Security Requirements for Signature Creation and Validation
EN	3	66	1	1	1	Protection Profiles for Signature Creation & Validation Applications
						Technical Specifications
EN	3	66	1	1	2	Procedures for Signature Creation and Validation
EN	3	66	1	2	2	CAdES - CMS Advanced Electronic Signature Formats
EN	3	66	1	3	2	XAdES - XML Advanced Electronic Signature Formats
EN	3	66	1	4	2	PAdES - PDF Advanced Electronic Signature Formats
EN	3	66	1	5	2	ASiC - Associated Signature Containers
EN	3	66	1	6	2	Signature Policies
						Conformance Assessment
EN	3	66	1	1	3	Conformance Assessment for Signature Creation & Validation Applications (& Procedures)
						Testing Compliance & Interoperability
TS	1	66	1	0	4	General requirements on Testing Compliance & Interoperability of SC&V
TS	1	66	1	2	4	CAdES Testing Compliance & Interoperability
TS	1	66	1	3	4	XAdES Testing Compliance & Interoperability
TS	1	66	1	4	4	PAdES Testing Compliance & Interoperability
TS	1	66	1	5	4	ASiC Testing Compliance & Interoperability
TS	1	66	1	6	4	Testing Compliance & Interoperability of Signature Policies

Guidance

TR 166 100 Business Driven Guidance for Signature Creation and Validation

This document provides business guidance for electronic signature standardisation from the viewpoint of signature creation and validation. The selection of standards resulting from this guidance has impact on the selection of standards in other areas (excluding trust applications using electronic signatures). Further information on the proposed approach to such business guidance is given in Annex B.

Policy and Security Requirements

EN 366 101 Policy and Security Requirements for Electronic Signature Creation and Validation

This document provides policy requirements for electronic Signature Creation and Validation (Applications). This would include procedural aspects that are not directly machine processable, as well as aspects which may be defined in a machine processable way (see EN 366 162).

This document will include a template for a **Human readable document** covering the rules to be applied on the electronic signatures to be considered in a business e-process environment.

NOTE 1: This will take into account the standards for Information Security Management Systems in ISO 27000 [i.10] and templates for practice statements as in RFC 3647 [i.11].

NOTE 2: The future work of the STF will be to further analyse this aspect in the gap analysis and recommend future work.

EN 366 111 Protection Profiles for Signature Creation & Validation Applications

This multi-part document specifies the security requirements for signature creation and verification applications. This includes security requirements on mandatory core functions of signature creation and verification applications as well as security requirements for possible extensions to the core functions.

Technical Specifications

EN 366 112 Procedures for Signature Creation and Validation

This document specifies procedures for creation and validation of an Advanced Electronic Signature within a given policy context. This document specifies support for validation of XAdES (XML Advanced Electronic Signature), CAdES (CMS Advanced electronic signature) and PAdES (PDF Advanced electronic signature) signatures taking into account use of Trust Lists.

EN 366 122 CMS Advanced Electronic Signature Formats (CAdES)

This document contains all the specifications related to Advanced Electronic Signatures built on top of CMS signatures by incorporation of signed and unsigned attributes. This is a multi-part document that includes the base specification and associated profiles.

This multi-part document includes:

- **CMS Advanced Electronic Signatures (CAdES)**. This document specifies the format for a set of attributes that are added to CMS signatures to become CMS Advanced Electronic Signatures. It also specifies requirements on their construction and incorporation to the signature as signed or unsigned attributes.
- **CAdES Baseline Profile**. This document specifies a profile identifying a common set of options that are appropriate for maximizing interoperability between CAdES signatures when they are used in the context of the EU Service Directive [i.15].
- **CAdES eInvoicing Profile**: This document specifies a profile identifying a common set of options for eInvoicing.

EN 366 132 XML Advanced Electronic Signature Formats (XAdES)

This document contains all the specifications related to Advanced Electronic Signatures built on top of XML signatures by incorporation of signed and unsigned properties. This is a multi-part document that includes the base specification and associated profiles.

This multi-part document includes:

- **XML Advanced Electronic Signatures (XAdES)**. This document specifies the format for a set of properties that are added to XML Signatures for becoming an XML Advanced Electronic Signature. It also specifies requirements on their construction and incorporation (distributed or not-distributed) to the signature as signed or unsigned properties.

NOTE 3: This will need to take account of updates to XMLDSig [i.12].

- **XAdES Baseline Profile**. This document specifies a profile identifying a common set of options that are appropriate for maximizing interoperability between XAdES signatures when they are used in the context of the EU Service Directive [i.15] .
- **XAdES eInvoicing Profile**: This document specifies a profile identifying a common set of options for eInvoicing.

EN 366 142 PDF Advanced Electronic Signature Formats (PAdES)

This document contains all the specifications related to Advanced Electronic Signatures embedded within PDF documents. This is a multi-part document that includes the base specification and associated profiles.

This multi-part document includes:

- **PAdES Overview – a framework document for PAdES**. This document provides a framework for the set of profiles for PAdES. It provides a general description of support for signatures in PDF documents including use of XML signatures to protect XML data in PDF documents; it also lists the features of the different profiles specified in other parts of the document; finally it describes how the profiles may be used in combination.

- **PAdES Basic - Profile based on ISO 32000-1** This document profiles the use of PDF signatures as described in ISO 32000-1 [i.13] and based on CMS, for its use in any application areas where PDF is the appropriate technology for **exchange** of digital documents including interactive forms.

- **PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles**. This document profiles the use of PDF Signatures specified in ISO 32000-1 with an alternative signature encoding to support signature formats **equivalent** to the signature forms CAdES-BES, CAdES-EPES and CAdES-T as specified in EN 366 122.

- **PAdES Long Term - PAdES-LTV Profile**. This document profiles the electronic signature formats found in ISO 32000-1 to support Long Term Validation (LTV) of PDF signatures. It specifies a profile to support the equivalent functionality to the signature forms CAdES-X Long and CAdES-A as specified in EN 366 122 in a single profile PAdES-LTV, by incorporation of newly specified PDF objects conveying the required validation material.

- **PAdES for XML Content - Profiles for XAdES signatures**. This document defines profiles for the usage of XAdES signatures, as defined in EN 366 132, for signing XML content within the PDF containers, including the following situations:

  - One XML document (compliant with an arbitrary XML language, like UBL for e-Invoicing) that is completely or partially signed with at least one enveloped XAdES signature and that is incorporated within a PDF container.

  - Signed (with XML Sig or XAdES signature) dynamic XFA forms.

- **Visual Representations of Electronic Signatures**. This document specifies requirements and recommendations for the visual representations of Advanced Electronic Signatures (AdES) in PDFs. This covers:

  - Signature appearance: The visual representation of the human act of signing placed within a PDF document at signing time and linked to an Advanced Electronic Signature.

  - Signature verification representation: The visual representation of the verification of an Advanced Electronic Signature.

- **PAdES Baseline Profile**. This document specifies a profile identifying a common set of options that are appropriate for maximizing interoperability between PAdES signatures when they are used in the context of the EU Service Directive.

- **PAdES eInvoicing Profile**: This document specifies a profile identifying a common set of options for eInvoicing.

EN 366 152 Associated Signature Containers (ASiC)

This document contains all the specifications related to the so-called Associated Signature Container. That is containers that bind together a number of signed data objects with Advanced Electronic Signatures applied to them or time-stamp tokens computed on them. This is a multi-part document that includes the mother specification and a baseline profile for it use in compliance with CD 2011/130/EU [i.14] in the context of the "Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market" [i.15] (EU Services Directive henceforth) and any context where similar requirements are present.

This multi-part document includes:

- **Associated Signature Containers (ASiC)**. This document specifies the format for a single container binding together a number of signed objects (e.g. documents, XML structured data, spreadsheet, multimedia content) with either Advanced Electronic Signatures or time-stamps. This uses package formats based on ZIP and supports the following signature and time-stamp token formats: CAdES signature(s) as specified in EN 366 122, XAdES detached signature(s) as specified in EN 366 132; and RFC 3161 [i.16] time-stamp tokens.

- **ASiC Baseline Profile**. This document specifies a profile identifying a common set of options that are appropriate for maximizing interoperability between ASiC containers when they are used in the context of the EU Services Directive.

- **ASiC eInvoicing Profile**: This document specifies a profile identifying a common set of options for eInvoicing.

EN 366 162 Signature Policies

This document fully addresses signature policies to be used in the management of electronic signatures within extended business models. This is a multi-part document whose internal structure is shown below:

- **Human readable format for Signature Policies**. This document elaborates the concept of signature policy documents, addresses relevant aspects of their usage, and specifies the constituent parts of a signature policy and their semantics. This provides a standardised table of content for human readable signature policies.

- **XML format for Signature Policies**. This document specifies a XML format for those parts of the Signature Policy that may be structured and are worth to be automatically processed by both signer and verifying applications. This document also specifies the processes to be performed by the aforementioned applications while using this format during the generation or the verification of electronic signatures.

- **ASN.1 format for Signature Policies**. This document specifies a XML format for those parts of the Signature Policy that may be structured and are worth to be automatically processed by both signer and verifying applications. This document also specifies the processes to be performed by the aforementioned applications while using this format during the generation or the verification of electronic signatures.

Conformance Assessment

EN 366 113 Conformance Assessment for Signature Creation and Validation Applications (& Procedures)

This document introduces the three aspects of assessment detailed in separate specifications:

a) Assessment of user environment against policy requirements: the conformance rules for assessing conformance of SCA or SVA against Policy Requirements. This will show the complete process for performing complete assessment and make some reference to other conformance assessment guidance (incl. technical specifications, protection profiles, signature policies.

b) Assessment of products and applications for electronic signature creation and validation against protection profiles.

c) Assessment of conformance to Advanced Electronic Signature formats and protocols.

d) Assessment of conformance of a specific machine processable signature policy to the business process policy requirements.

NOTE 4: Assessment may require use of testing compliance or interoperability.

Testing Compliance & Interoperability

TS 166 104 General requirements on Testing Compliance & Interoperability of Signature Creation and Validation

This set of documents specifies general requirements for testing compliance and interoperability of signature creation and validation applications.

As a general principle, EN 366 **x**04 documents are meant to group common requirements to all potential sub-parts with regards to testing compliance & interoperability. It could also be used as an introductory document to how testing compliance & integrity is dealt with in the sub-areas (e.g. general principles and requirements for PlugTests).

TS 166 124 CAdES Testing Compliance & Interoperability

This document provides technical specifications for helping implementers and accelerating the development of CAdES signature creation and validation applications. The test results may also be used in conformance assessment for signature creation and validation applications (EN 366 113) with policies requiring conformity to CAdES formats and procedures. First, it will define test suites as completely as possible for supporting the organization of interoperability testing events where different CAdES related applications may check their actual interoperability. Additionally, it will include the specifications required for building up software tools for actually testing technical compliance of CAdES signatures against the relevant CAdES related technical specifications.

This is a multipart document covering the following topics:

- **Test suites for testing interoperability of CAdES signatures**. This document would be used for those entities interested in testing the interoperability of tools that generate and verify CAdES signatures not adhering to any specific profile, but compliant with the mother CAdES specification as defined in EN 366 122.
- **Test suites for testing interoperability of Baseline CAdES signatures**. This document would be used for those entities interested in testing the interoperability of tools that generate and verify CAdES signatures that claim to be compliant with the CAdES Baseline Profile as specified in EN 366 122.
- **Specifications for testing compliance of CAdES Signatures**. This document will specify, among other things, rules for testing compliance of signatures against the CAdES specification. It should allow developing a tool that could automatically check that the CAdES signatures generated by a certain tool are fully compliant with the relevant aforementioned specifications, without claiming any statement on their validity or not.
- **Specifications for testing compliance of Baseline CAdES Signatures**. This document will specify, among other things, rules for testing compliance of signatures against the CAdES Baseline Profile specification. It should allow developing a tool that could automatically check that the CAdES Baseline signatures generated by a certain tool are fully compliant with the relevant aforementioned specifications, without any statement on their validity.
- **Specifications for testing compliance of CAdES Signatures validation**. This should allow developing a tool that could automatically check that the generated CAdES signatures are fully compliant with the relevant aforementioned specifications and validate the signature according to EN 366 112.

TS 166 134 XAdES Testing Compliance & Interoperability

This document provides technical specifications for helping implementers and accelerating the development of XAdES signature creation and validation applications. The test results may also be used in conformance assessment for signature creation and validation applications (EN 366 113) with policies requiring conformity to XAdES formats and procedures. First, it will define test suites as completely as possible for supporting the organization of interoperability testing events where different XAdES related applications may check their actual interoperability. Additionally, it will include the specifications required for building up software tools for actually testing technical compliance of XAdES signatures against the relevant XAdES related technical specifications.

This is a multipart document structured as follows:

- **Test suites for testing interoperability of XAdES signatures**. This document would be used for those entities interested in testing tools that generate and verify XAdES signatures not adhered to any specific profile, but compliant with the mother XAdES specification as defined in EN 366 132.
- **Test suites for testing interoperability of Baseline XAdES signatures**. This document would be used for those entities interested in testing tools that generate and verify XAdES signatures that claim to be compliant with the XAdES Baseline Profile as specified in EN 366 132.
- **Specifications for testing compliance of XAdES Signatures**. This document will specify, among other things, rules for testing compliance of signatures against the XAdES specification It should allow developing a tool that could automatically check that generated XAdES signatures are fully compliant with the relevant aforementioned specifications, without any statement on their validity.
- **Specifications for testing compliance of Baseline XAdES Signatures**. This document will specify, among other things, rules for testing compliance of signatures against the XAdES specification. It should allow developing a tool that could automatically check that the XAdES Baseline signatures generated by a certain

tool are fully compliant with the relevant aforementioned specifications, without claiming any statement on their validity or not.

- **Specifications for testing compliance of XAdES Signatures validation**. This should allow developing a tool that could automatically check that the XAdES signatures generated by a certain tool are fully compliant with the relevant aforementioned specifications and validate the signature according to EN 366 112.

TS 166 144 PAdES Testing Compliance & Interoperability

This document provides technical specifications for helping implementers and accelerating the development of PAdES signature creation and validation applications. The test results may also be used in conformance assessment for signature creation and validation applications (EN 366 113) with policies requiring conformity to PAdES formats and procedures. First, it will define test suites as completely as possible for supporting the organization of interoperability testing events where different PAdES related applications may check their actual interoperability. Additionally, it will include the specifications required for building up software tools for actually testing technical compliance of PAdES signatures against the relevant PAdES related technical specifications.

This is a multipart document structured as follows:

- **Test suites for testing interoperability of PAdES signatures**. This document would be used for those entities interested in testing tools that generate and verify PAdES signatures not adhered to any specific profile, but compliant with the mother PAdES specification as defined in EN 366 142.

- **Test suites for testing interoperability of Baseline PAdES signatures**. This document would be used for those entities interested in testing tools that generate and verify PAdES signatures that claim to be compliant with the PAdES Baseline Profile as specified in EN 366 142.

- **Specifications for testing compliance of PAdES Signatures**. This document will specify, among other things, rules for testing compliance of signatures against the PAdES specification. It should allow developing a tool that could automatically check that generated PAdES signatures are fully compliant with the relevant aforementioned specifications, without any statement on their validity.

- **Specifications for testing compliance of Baseline PAdES Signatures**. This document will specify, among other things, rules for testing compliance of signatures against the PAdES Baseline Profile specification. It should allow developing a tool that could automatically check that the PAdES Baseline signatures generated by a certain tool are fully compliant with the relevant aforementioned specifications, without claiming any statement on their validity or not.

- **Specifications for testing compliance of PAdES Signatures validation**. This should allow developing a tool that could automatically check that the PAdES signatures generated by a certain tool are fully compliant with the relevant aforementioned specifications and validate the signature according to EN 366 112.

TS 166 154 ASiC Signature Testing Compliance & Interoperability

This document provides technical specifications for helping implementers and accelerating the development of ASiC containers creation and validation applications. The test results may also be used in conformance assessment for signature creation and validation applications (EN 366 113) with policies requiring conformity to ASiC formats and procedures. First, it will define test suites as much complete as possible for supporting the organization of interoperability testing events where different ASiC container related applications may check their actual interoperability. Additionally, it will include the specifications required for building up software tools for actually testing technical compliance of ASiC signatures against the relevant ASiC container related technical specifications.

This is a multipart document covering the following topics:

- **Test suites for testing interoperability of ASiC Signatures**. This document would be used for those entities interested in testing tools that generate and verify ASiC signatures not adhered to any specific profile, but compliant with the mother ASiC specification as defined in EN 366 152.

- **Test suites for testing interoperability of Baseline ASiC Signatures**. This document would be used for those entities interested in testing tools that generate and verify ASiC signatures that claim to be compliant with the ASiC Baseline Profile as specified in EN 366 152.

- **Specifications for testing compliance of ASiC Signatures**. This document will specify, among other things, rules for testing compliance of signatures against the ASiC specification. It should allow developing a tool that

could automatically check that generated ASiC signatures are fully compliant with the relevant aforementioned specifications, without any statement on their validity.

- **Specifications for testing compliance of Baseline ASiC Signatures**. This document will specify, among other things, rules for testing compliance of signatures against the ASiC specification. It should allow developing a tool that could automatically check that the ASiC Baseline signatures generated by a certain tool are fully compliant with the relevant aforementioned specifications, without claiming any statement on their validity or not.

- **Specifications for testing compliance of ASiC Signatures validation**. This should allow developing a tool that could automatically check that the ASiC signatures generated by a certain tool are fully compliant with the relevant aforementioned specifications and validate the signature according to EN 366 112.

EN 366 164 Testing Compliance & Interoperability of Signature Policies

This document provides technical specifications for helping implementers and accelerating the development of Signature Policies. The test results may also be used in conformance assessment for signature creation and validation applications (EN 366 113) with policies requiring conformity to machine processable Signature Polices format specifications.

First, it will define test suites as much complete as possible for supporting the organization of interoperability testing events where different Signature Policy based applications may check their actual interoperability.

Additionally, it will include the specifications required for building up software tools for actually testing technical compliance of machine processable Signature Policies against the relevant technical specifications.

5.3.3 Signature Creation Devices

The documents for electronic signature standardisation for signature creation devices are summarised in table 2 with further details provided below:

Table 2: Standards for Signature Creation Devices

			Signature Creation Devices			
				Sub-areas		
					Guidance	
TR	1	66	2	0	0	Business Driven Guidance for Signature Creation Devices
					Policy & Security Requirements	
EN	3	66	2	1	1	Protection Profiles for Secure Signature Creation Devices
EN	3	66	2	2	1	Protection Profiles for Signature Creation Devices used by TSPs
EN	3	66	2	3	1	Protection Profiles for other Signature Creation Devices
					Technical Specifications	
EN	3	66	2	1	2	APIs for SSCDs
					Conformance Assessment	
EN	3	66	2	0	3	General requirements for Signature Creation Device Conformance Assessment
EN	3	66	2	1	3	Conformance Assessment for SSCDs
EN	3	66	2	2	3	Conformance Assessment for Signature Creation Devices used by TSPs
EN	3	66	2	3	3	Conformance Assessment for other Signature Creation Devices
					Testing Compliance & Interoperability	
-		-	-	-	-	*no requirement identified*

Guidance

TR 166 200 Business Driven Guidance for Signature Creation Devices

This document provides guidance for the selection of standards for electronic signature devices for given business requirements.

Policy & Security Requirements

EN 366 201 Policy and Security Requirements for Signature Creation Devices

No requirement has been identified for this type of document.

EN 366 211 Protection Profiles for Secure Signature Creation Devices

This document specifies the security requirements for a SSCD which is the target of evaluation. It follows the rules and formats of the Common Criteria v3 [i.17].

This is a multi-part document covering the following topics:

- **Overview:** An introduction to the SSCD protection profiles.
- **Device with key generation**: This document specifies a protection profile for an SSCD that performs its core operations including the generation of signature keys in the device. This profile may be extended through extensions specified in other parts.
- **Device with key import:** This document specifies a protection profile for an SSCD that performs its core operations including import of the signature key generated in a trusted manner outside the device.
- **Extension for device with key generation and trusted communication with certificate generation application:** This document specifies an extension protection profile for an SSCD with key generation that support establishing a trusted channel with a certificate-generating application. This profile may be extended through extensions specified in other parts.
- **Extension for device with key generation and trusted communication with signature creation application:** This document specifies an extension protection profile for an SSCD with key generation that additionally supports establishing a trusted channel with a signature-creation application.
- **Extension for device with key import and trusted communication with signature creation application**: This document specifies an extension protection profile for an SSCD with key import that additionally supports establishing a trusted channel with a signature-creation application.

EN 366 221 Protection Profiles for Signature Creation Devices used by TSPs

This document specifies security requirements for cryptographic devices used by Trust Service Providers including Trust Applications using Electronic Signatures and TSPs supporting electronic signatures. It follows the rules and formats of the Common Criteria v3 [i.17].

This is a multi-part document covering the following topics:

- **Protection Profile for cryptographic module for TSP signing operations with backup**: This document defines the security requirements of a Cryptographic Module used by a TSP as part of its trustworthy system to provide services which involve signature creation, such as Qualified Certificate Issuance Services or Time-Stamping services. The cryptographic module, which is the Target of Evaluation (TOE), is used for the creation of TSP key pairs, and their usage for the creation and verification of Advanced Electronic Signatures in qualified certificates or certificate status information.
- **Protection Profile for TSP key generation services**: This document defines the security requirements of a Cryptographic Module used by TSP as part of its trustworthy system to provide Key Generation Services. The Cryptographic Module, which is the Target of Evaluation (TOE), is used for the creation of subscriber private keys, and loading them into Secure Signature Creation Devices as part of a Subscriber Device Provision Service.
- **Protection Profile for cryptographic module for TSP signing operations:** This document defines the security requirements of a Cryptographic Module used by TSP as part of its trustworthy system to provide services which involve signature creation, such as Qualified Certificate issuance services or Time-Stamping services. The Cryptographic Module, which is the Target of Evaluation is used for the creation of TSP key pairs, and their usage for the creation and verification of Advanced Electronic Signatures in qualified certificates or certificate status information.

EN 366 231 Protection Profiles for other Signature Creation Devices

This document specifies the security requirements for other Signature Creation Devices which are the TOE. It is following the rules and formats of the Common Criteria v3 [i.17]. Whilst the focus often has been on "Qualified Electronic Signatures" as specified in Article 5.1 of Directive 1999/93/EC [i.1], a side effect was that the requirements of employing general Electronic Signatures (referred to as "5.2 signatures") in e-commerce were not sufficiently addressed. The purpose of this document is to specify the security requirements for a signature-creation device that can be implemented for such Article 5.2 signatures, and thus fulfil a wider market need than the "Secure Signature-Creation

Device" required for Qualified Electronic Signatures. This document contains one or more Protection Profile for a Signature Creation Device suitable for such general electronic signatures.

NOTE 1: This may be organised as a multipart document in order to cover, amongst other types of devices, devices for natural person other than SSCDs, and devices for legal persons, HSMs and potentially software based signature creation devices. To date the structure and organisation of such parts and multi-parts as well as the need for additional ENs is yet to be defined.

Technical specifications

EN 366 212 APIs for Secure Signature Creation Devices

This standard describes an application interface and behaviour of the SSCD in the context of Identification, Authentication and Electronic Signature (IAS) services.

This is a multi-part document covering the following topics

- **Basic services**: This specifies mandatory mechanisms for smart cards to be used as SSCD, and covers user verification, signature creation, device authentication, password-based mechanisms, establishment of a secure channel and key generation.
- **Additional services**: This specifies mechanisms to support services around Identification, Authentication and Digital Signature (IAS) services in addition to the SSCD mechanisms already described in Part 1 to enable interoperability and usage for IAS services on a national or European level. It also specifies additional mechanisms like Client/Server authentication, role authentication, symmetric key transmission between a remote server and a smart card, signature verification, identity management and privacy mechanisms.

Conformance Assessment

EN 366 203 General requirements for Signature Creation Device Conformance Assessment

This document provides the rationale for the guidance on conformity assessment concerning the services, processes, systems and products around electronic signature. This document is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories.

NOTE: This is to be based around the existing Common Criteria [i.17] evaluation schemes.

EN 366 213 Conformance Assessment for Secure Signature Creation Devices

The purpose of this document is to provide guidance with a view to harmonise the assessment of the standards implementation for services, processes, systems and products for Electronic Signatures. In particular, this document provides guidance on conformance assessment of Secure Signature Creation Devices against **EN 366 211.**

EN 366 223 Conformance Assessment for Signature Creation Devices used by TSPs

This document provides guidance on conformance assessment of signature creation devices (cryptographic modules) used by TSPs for signing operations and key generation services against **EN 366 221.**

EN 366 233 Conformance Assessment for Other Signature Creation Devices

This document provides guidance on conformance assessment of other Signature Creation devices against **EN 366 231**.

NOTE 2: This may be organised as a multi-part document in order to cover, amongst other types of devices, natural person devices that are not SSCDs, entity (non natural persons) HSMs and software based signature creation devices. To date the structure and organisation of such parts and multi-parts as well as the need for additional ENs is yet to be defined.

Technical Compliance & Interoperability Testing

EN 366 204

No requirements identified so far for such a document.

5.3.4 Cryptographic Suites

The documents for electronic signature standardisation for cryptographic suites are summarised in table 3 with further details provided below:

Table 3: Standards for Cryptographic Suites

			Cryptographic Suites			
			Sub-areas			
				Guidance		
TR	1	66	3	0	0	Business Driven Guidance for Cryptographic Suites
				Technical Specifications		
EN	3	66	3	1	2	Cryptographic Suites for Secure Electronic Signatures
				Testing Compliance & Interoperability		
TS	1	66	3	1	4	Testing of implementations of cryptographic algorithms

Guidance

TR 166 300 Business Driven Guidance for Cryptographic Suites

This document provides guidance for the selection of cryptographic **suites** for given business requirements.

NOTE: Regular maintenance of cryptographic suites specifications should be ensured and mechanisms for ensuring this should be proposed and implemented.

Technical Specifications

TS 166 312 Cryptographic Suites for Secure Electronic Signatures

This document defines a number of cryptographic suites for secure electronic signatures including a list of hash functions and a list of signature schemes, as well as the recommended combinations of hash functions and signatures in the form of "signature suites" to support Advanced Electronic Signatures.

Technical Compliance & Interoperability Testing

TS 166 314 Testing of implementations of Cryptographic algorithms

This document covers the specifications of testing and validation of the functional behaviour of the cryptographic algorithms.

5.3.5 TSPs Supporting Electronic Signatures

The documents for electronic signature standardisation for TSP Supporting Electronic Signature are summarised in table 4 with further details provided below:

Table 4: Standards for TSPs supporting Electronic Signatures

			TSPs Supporting Electronic Signatures			
			Sub-areas			
				Guidance		
TR	1	66	4	0	0	Business Driven Guidance for TSPs Supporting Electronic Signatures
				Policy & Security Requirements		
EN	3	66	4	0	1	General Policy & Security Requirements for TSPs Supporting Electronic Signatures
EN	3	66	4	1	1	Policy & Security Requirements for TSPs Issuing Qualified Certificates
EN	3	66	4	2	1	Policy & Security Requirements for TSPs issuing Public Key Certificates
EN	3	66	4	3	1	Policy & Security Requirements for TSPs providing Time-Stamping Services
EN	3	66	4	4	1	Policy & Security Requirements for TSPs providing Signature Generation Services
EN	3	66	4	5	1	Policy & Security Requirements for TSPs providing Signature Validation Services
				Technical Specifications		
EN	3	66	4	1	2	Profiles for TSPs issuing Qualified Certificate
EN	3	66	4	2	2	Profiles for TSPs issuing Public Key Certificates
EN	3	66	4	3	2	Profiles for TSPs providing Time-Stamping services
EN	3	66	4	4	2	Profiles for TSPs provding Signature Generation Services
EN	3	66	4	5	2	Profiles for TSPs providing Signature Validation Services
				Conformance Assessment		
EN	3	66	4	0	3	General requirements and guidance for Conformance Assessment of TSPs supporting e-Signatures
EN	3	66	4	1	3	Conformance Assessment for TSPs Issuing Qualified Certificates
EN	3	66	4	2	3	Conformance Assessment for TSPs Issuing Public Key Certificates
EN	3	66	4	3	3	Conformance Assessment for TSPs providing Time-Stamping Services
EN	3	66	4	4	3	Conformance Assessment for TSPs providing Signature Generation Services
EN	3	66	4	5	3	Conformance Assessment for TSPs providing Signature Validation Services
				Testing Compliance & Interoperability		
-		-	-	-	-	*no requirement identified for such a document*

Guidance

TS 166 400 Business Driven Guidance for TSPs Supporting Electronic Signatures

This document provides guidance for the selection of standards for TSPs for given business requirements.

NOTE 1: When there would be a need for identifying and producing specific Business Driven Guidance for specific types of TSPs supporting electronic signatures, the Rationalised Framework model allows usage of 66 410, 66 420, 66 430, etc. documents for such purpose.

Policy & Security Requirements

EN 366 401 General Policy & Security Requirements for TSPs Supporting Electronic Signatures

This document specifies policy and security requirements for TSPs Supporting Electronic Signatures that are independent of the type of TSP.

This document specifies security requirements for TSP Systems. This multipart document includes:

- **General part.**
- **Security requirements for trustworthy systems managing certificates for electronic signatures**: This document is specifically relevant for manufacturers of Trustworthy Systems used for managing certificates, but may be adopted by anyone deploying trusted systems and wanting to meet the requirements of [Directive 1999/93/EC]. It provides an overview of a TSP system broken down into a number of mandatory (core) or optional (supplementary) services.
- **Security requirements for trustworthy systems for provisioning of time-stamping services**
- **Security requirements for trustworthy systems for Signature Generation services**
- **Security requirements for trustworthy systems for Signature Verification services**

EN 366 411 Policy & Security Requirements for TSPs Issuing Qualified Certificates

This document specifies policy requirements for TSPs issuing qualified certificates. It references EN 366 401 for generic requirements.

EN 366 421 Policy & Security Requirements for TSPs Issuing Public Key Certificates

This document specifies policy requirements for TSPs issuing public key certificates other than qualified certificates. It references EN 366 401 for generic requirements.

EN 366 431 Policy & Security Requirements for TSPs providing Time-Stamping Services

This document specifies policy requirements for TSPs providing Time-stamping services based on RFC 3161 [i.16]. It references EN 366 401 for generic requirements.

EN 366 441 Policy & Security Requirements for TSPs providing Signature Generation Services

This document specifies policy requirements for TSPs providing signature generation services. It references EN 366 401 for generic requirements.

EN 366 451 Policy & Security Requirements for TSPs providing Signature Validation Services

This document specifies policy requirements for TSPs providing Signature Validation Services. It references EN 366 401 for generic requirements.

Technical Specifications

EN 366 412 Profiles for TSPs issuing Qualified Certificates

This document provides specifications for specific profiles applicable to TSPs issuing qualified certificates. This includes notably specifications of a profile for the use of public key certificates, as specified in ITU-T X.509 [i.18], for use as qualified certificates.

EN 366 422 Profiles for TSPs issuing Public Key Certificates

This (multipart) document provides specifications for specific profiles applicable to TSPs issuing public key certificates that are not qualified certificates.

EN 366 432 Profiles for TSPs providing Time-Stamping Services

This document specifies a profile for the format and procedures for time-stamping as specified in RFC 3161 [i.16].

EN 366 442 Profiles for TSPs providing Signature Generation Services

This document specifies a profile for the format and procedures for TSPs providing Signature Generation Services.

EN 366 452 Profiles for TSPs providing Signature Validation Services

This document specifies a profile for the format and procedures for TSPs providing Signature Validation Services.

Conformance Assessment

EN 366 403 General requirements and guidance for Conformance Assessment of TSPs Supporting Electronic Signatures

This document specifies general requirements for conformance assessment independent of the form of TSP and provides guidance for the supervision and assessment of a TSP supporting electronic signatures.

EN 366 413 Conformance Assessment for TSPs Issuing Qualified Certificates

This document specifies requirements and provides guidance for the supervision and assessment of a TSP issuing qualified certificates.

NOTE 2: It may be assumed that any requirement relating to completion of conformity testing might be covered here and reference the appropriate Technical Conformity & Interoperability Testing documents.

EN 366 423 Conformance Assessment for TSPs Issuing Public Key Certificates

This document specifies requirements and provides guidance for the supervision and assessment of a Certification Authority issuing public key certificates other than qualified

EN 366 433 Conformance Assessment for TSPs providing Time-Stamping Services

This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing time-stamping services.

EN 366 443 Conformance Assessment for TSPs providing Signature Generation Services

This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing Signature Generation Services.

EN 366 453 Conformance Assessment for TSPs providing Signature Validation Services

This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing Signature Validation Services.

Testing Compliance & Interoperability

Not applicable so far.

NOTE 3: At the current date, no requirement for such documents has been identified. It may however be the case that specifications for conformance checker tools could be identified in the future such as conformance checker for generated Trust Service tokens such as qualified certificates, public key certificates against a specific profile, or time-stamp tokens.

5.3.6 Trust Application Service Providers

The documents for electronic signature standardisation for Trust Application Service providers are summarised in table 5 with further details provided below:

Table 5: Standards for Trust Application Service Providers

			Trust Application Service Providers			
			Sub-areas			
				Guidance		
TR	1	66	5	0	0	Business Driven Guidance for Trust Application Service Providers
				Policy & Security Requirements		
EN	3	66	5	0	1	General Policy & Security Requirements for Trust Application Service Providers
EN	3	66	5	1	1	Policy & Security Requirements for Registered Electronic Mail (REM) and Registered Electronic Delivery (RED)
EN	3	66	5	2	1	Policy & Security Requirements for Information Preservation Service Providers (IPSPs)
				Technical Specifications		
EN	3	66	5	1	2	Registered Electronic Mail (REM) and Registered Electronic Delivery (RED) Services
EN	3	66	5	2	2	Information Preservation Services through signing
				Conformance Assessment		
EN	3	66	5	0	3	General requirements and guidance for Conformance Assessment of TASPs
EN	3	66	5	1	3	Conformance Assessment of REM and RED Service Providers
EN	3	66	5	2	3	Conformance Assessment of Information Preservation Service Providers
				Testing Compliance & Interoperability		
TS	1	66	5	0	4	General requirements for Testing Compliance & Interoperability of TASPs
TS	1	66	5	1	4	Testing Compliance & Interoperability of REM and RED Service Providers

Guidance

TR 166 500 Guidance for Trust Application Service Provider

This document provides guidance for the selection of standards for trusted application service providers for given business requirements.

The document identifies a number of relevant Trusted Application Services using electronic signatures in different business areas, and whose provision has already been standardized. Additionally, for each of the services, it provides guidance for the selection of the suitable standards, ensuring in this way their correct provision and interoperability across the European Union.

Policy & Security Requirements

EN 366 501 General Policy & Security Requirements for Trust Application Service Providers

This document specifies policy requirements that are common to trust application services, and whose provision has been standardized and that requires intensive usage of electronic signatures.

NOTE 1: Whether "Security requirements for TASP Trustworthy systems" should be merged within those general policy & security requirements is yet to be further analysed.

(Sub)part: Security requirements for TASP Trustworthy Systems

This document specifies security requirements for TASP Systems. This multipart document includes:

- **General part.**
- **Security requirements for trustworthy systems used for the provision of REM & RED services**
- **Security requirements for trustworthy systems used for the provision of information preservation services**

EN 366 511 Policy & Security Requirements for Registered Electronic Mail (REM) and Registered Electronic Delivery (RED) Service Providers

This document specifies policy requirements for REM & RED service providers required to be recognized as a provider of this type of services. It might define different conformance levels for each style of operation and the corresponding set of requirements to be satisfied in each level. This document also addresses requirements on Information Security Management and Security requirements for TASP trustworthy systems (EN 366 502). It references EN 366 501 for generic requirements.

EN 366 521 Policy & Security Requirements for Information Preservation Service Providers (IPSPs)

This document specifies policy requirements for IPSPs. It references EN 366 501 for generic requirements.

This document also references the Security requirements for TASP trustworthy systems (EN 366 502) and may address specific Information Security Management Systems or Information Preservation Systems, by specifying specific security requirements for Information Preservation Service Providers to abide by, when implementing and managing an IPS, in order to provide Information Preservation Services that are trustable and reliable from the Information Security viewpoint. This document does not address any archival specific issues, like definition of information metadata structure and methods to build them, links between information to implement virtual folders, etc.

Technical Specifications

EN 366 512 Registered Electronic Mail and Registered Electronic Delivery Services

This document provides technical specifications for the provision of Registered Electronic Mail and Registered Electronic Delivery services, i.e., services that in addition to deliver data objects to purported recipients, are also entitled to provide to both sender and recipient(s) a set of reliable electronic evidence that prove that certain relevant events have actually taken place (submission by the sender, delivery by the provider to the recipient, retrieval by the recipient, etc.) and that have legal value. This is a multi-part document whose structure is detailed below:

- **Framework, Architecture and Evidence**. This is a document structured in three sub-parts, whose structure is detailed below:
  - **Registered Electronic Mail and Electronic Delivery Overview – a framework document**. This document provides an overview of the whole set of specifications included in the Technical Specification
  - **Architecture**. This document provides an overall view of the standardized service, addressing the following aspects:
    - Logical model, namely: components, styles of operation, Roles within a service provider, grouping of providers in administrative domains;
    - Interfaces between the different roles and providers;
    - Relevant events in the data objects flows and the corresponding evidence;
    - Trust building among providers pertaining to the same or to different administrative domains.

- **Evidence semantics and format**. This document fully specifies the set of evidence managed in the context of the service provision. The document fully specifies the semantics, the components, and the components' semantics for all the evidence. The document also specifies different formats for all the evidence in different syntax, namely: XML, ASN.1 and PDF.

- **Messages formats and bindings**. This part specifies different formats for the messages and the different bindings for different transport protocols. This is a document structured in two sub-parts, as detailed below:
  - **SMIME on SMTP**. This document specifies the format of the data objects when SMIME structures are used for conveying them, and when the transport protocol used is SMTP.
  - **SOAP on HTTP**. This document specifies the format of data objects when SOAP structures are used for conveying them, and when the transport protocol used is HTTP.
- **Interoperability profiles**. This part contains several sub-parts. Each sub-part specifies profile(s) for seamless exchange of data objects across providers that use different formats and/or transport protocols.

NOTE 2: Its internal structure will very much depend on the different relevant systems specified and built across the EU, as during the last years a number of specifications and non interoperable systems based on them, have been developed.

EN 366 522 Information Preservation Services through signing

This document specifies technical requirements for services providing document signing in support of information preservation. It specifies the requirements on the use of electronic signatures and time-stamping to maintain the authenticity and integrity of documents when stored over long periods. This can be applied to a single document or a set of documents, including multi-media objects, held in a container.

Conformance Assessment

EN 366 503 General requirements and guidance for Conformance Assessment of Trust Application Service Providers

This document specifies general requirements and provides guidance for the supervision and assessment of Trust Application Service Providers.

EN 366 513 Conformance Assessment of Registered Electronic Mail and Registered Electronic Delivery Service Providers

This document specifies requirements and provides guidance for the supervision and assessment of a Registered Electronic Mail and Registered Electronic Delivery Service Provider.

This document will provide a common set of criteria to assess implemented security and policy requirements against EN 366 511, usable by assessors.

EN 366 523 Conformance Assessment of Information Preservation Service Providers

This document specifies requirements and provides guidance for the supervision and assessment of an IPSP.

This document will provide a common set of criteria to review implemented security and policy requirements as per EN 366 521, usable by assessors of Information Preservation Systems.

Testing Compliance & Interoperability

TS 166 504 General requirements for Technical Conformity & Interoperability Testing for Trust Application Service Providers

This document specifies general requirements for specifying technical conformity and interoperability testing for TASPs.

TS 166 514 Testing Compliance & Interoperability of Registered Electronic Mail and Registered Electronic Delivery Service Providers

This document defines test suites that support interoperability tests among entities that plan to provide this type of services. This is a multi-part document, whose structure is detailed below:

- **Test suites for interoperability testing of providers using same format and transport protocols**. This document would be used for those providers that implement the service provision using the same combination of format and transport protocols, i.e. there will be two test-suites one for the providers using SMIME on SOAP and another for those using SOAP on HTTP.

- **Test suites for interoperability testing of providers using different format and transport protocols.** This document would be used for those providers that implement the service provision using different combinations of format and transport protocols. This document would define test-suites for the interoperability profiles for REM and RED.

- **Testing compliance**: This document specifies the tests to be performed for checking conformance against EN 366 512. This should allow to develop a tool that could automatically check that the messages and evidence set generated by a certain provider are fully compliant with the relevant aforementioned specifications.

5.3.7 Trust Service Status Lists Providers

Table 6: Standards for Trust Service Status (Lists) Providers

			Trust	Service Status Lists Providers		
				Sub-areas		
					Guidance	
TR	1	66	6	0	0	Business Driven Guidance for Trust Service Status Lists Providers
					Policy & Security Requirements	
EN	3	66	6	0	1	General Policy & Security Requirements for Trust Service Status Lists Providers
EN	3	66	6	1	1	Policy & Security Requirements for Trusted Lists Providers
					Technical Specifications	
EN	3	66	6	0	2	Trust Service Status Information Formats
EN	3	66	6	1	2	Trusted Lists
					Conformance Assessment	
EN	3	66	6	0	3	General requirements and guidance for Conformance Assessment of TSSLPs
EN	3	66	6	1	3	Conformance Assessment of Trusted List Providers
					Testing Compliance & Interoperability	
TS	1	66	6	0	4	General requirements for Testing Compliance & Interoperability of TSSLPs
TS	1	66	6	1	4	Testing Compliance & Interoperability of Trusted Lists

Guidance

TR 166 600 Business Driven Guidance for Trust Status Providers

This document provides guidance for the selection of standards for Trusted Service Status Lists Providers for given business requirements.

Policy & Security Requirements

EN 366 601 General Policy & Security Requirements for Trust Service Status Providers

This document specifies general policy requirements for providers issuing status information of trusted services. It will describe different models on which such providers may operate, how this influences the way the content of the lists should be interpreted and specific criteria for the provision of revisions to TSL information, which should be published by the providers.

EN 366 611 Policy & Security Requirements for Trusted Lists Providers

This document specifies specific policy requirements for issuers of Trusted List as they are defined in CD 2009/767/EC [i.19] as amended by CD 2010/425/EU [i.20].

Technical Specifications

EN 366 602 Trust-service Status Information Formats

This document contains all the specifications related to Trust-service Status Information Formats (Trust Service Lists). This is a multi-part document that includes the mother specification for Trust Service Status Lists (TSLs).

The structure of this multi-part document is shown below:

- **Trust-service Status Information Structure**
  This part specifies the Trust-service Status List structure. Each of the fields within the TSL is described to a level of detail sufficient to derive a consistent format specification.

- **ASN.1 Representation of Trust-service Status Information**
  This part specifies the ASN.1 structures to be used when implementing an ASN.1-version of TSLs.

- **XML Representation of Trust-service Status Information**
  This part specifies the XML structures to be used when implementing an XML-version of TSLs.

EN 366 612 Trusted Lists

This document contains all the specifications related to Trusted Lists for their use in the context of the Services Directive 2006/123/EC [i.15] and as they are defined in CD 2009/767/EC [i.19] amended by CD 2010/425/EU [i.20]. This is a multi-part document that defines the EN 366 602 baseline specifications for Trusted Lists. It specifies a profile identifying a common set of options that are appropriate for maximizing interoperability between issued TSLs when they are used in the context of the EU Service Directive and any context where similar requirements are present.

NOTE: As conceptually TSL can be used for providing status information on the approval of any type of provision of any type of Trust Service Token by any type of Trust Service Provider, the document structure proposed here is flexible enough to allocate sub-areas to determined categories of such services. As an example, TSL could be used for publishing in a EU-wide common way, the status of the determination of conformity of a signature creation device against the requirements laid down in Annex III of Directive 1999/93/EC [i.1] (SSCD) made by a Member State Designated Body. It is likely that for such a purpose, a specific baseline profile of TSL specifications as per EN 366 602 would be required.

Conformance Assessment

EN 366 603 General requirements and guidance for Conformance Assessment of TSSLPs

This document provides the rationale, rules and guidance on conformance assessment concerning the processes and products around the issuance and processing of Trust Service Status Lists.

EN 366 613 Conformance Assessment of Trusted Lists Providers

This document specifies the specific conformance rules for assessing conformance against EN 366 612 specifications related to both their generation and verification.

Testing Compliance & Interoperability

TS 166 604 General requirements for Testing Compliance & Interoperability of TSSLPs

This document specifies general requirements for specifying technical compliance and interoperability testing for TSSLPs. This may include test suites and specifications for conformity testing tools testing ASN.1 and /or XML representation of TSLs. This document will be used by those entities interested in testing tools that generate and verify Trust Service Status Lists in their ASN.1 or XML representation compliant with the specification EN 366 602. This is a multipart document that includes:

- Testing specifications for technical compliance & interoperability testing of ASN.1 representation of the Trust Service Status Lists: This document will be used by those entities interested in testing tools that generate and verify Trust Service Status Lists in its ASN.1 representation compliant with the specification EN 366 602.

- Testing specifications for technical compliance & interoperability testing of XML representation of the Trust Service Status Lists: This document will be used by those entities interested in testing tools that generate and verify Trust Service Status Lists in their XML representation compliant with the specification EN 366 602.

TS 166 614 Test suites and tests specifications for Technical Conformity & Interoperability Testing of Trusted Lists

This document provides technical specifications for helping implementers and accelerating the development of tools for creating and issuing Trusted Lists. First, it will define test suites as completely as possible for supporting the organization of interoperability testing events where different Trusted List related applications may check their actual

interoperability. Additionally, it will include the specifications required for building up software tools for actually testing technical compliance of Trusted Lists against the relevant Trusted List related technical specifications.

- **Test suites for testing interoperability of XML representation of Trusted Lists**. This document will be used by those entities interested in testing tools that generate and verify Trusted Lists in their XML representation compliant with EN 366 612.
- **Specifications for testing compliance of XML representation of Trusted Lists**. This document will specify, among other things, rules for testing compliance of Trusted Lists against Trusted List specifications. It should include not only rules for the static aspects of the Trusted Lists, i.e., the contents of a certain instantiation of the Trusted List, but also rules for testing dynamic aspects of the Trusted List, i.e. specific relationships among elements present in consecutive instantiations of one Trusted List as a result of certain very well specified events (Trusted List life cycle-related rules). It should allow developing a tool that could automatically check that the Trusted Lists generated by a certain tool are fully compliant with the relevant aforementioned specifications.

6 Gap Analysis

[To be written in next phase: The inventory of existing standards will be analysed against the rationalised framework to identify areas where further work is required to provide standards and guidelines to fit the framework]

7 Work Plan

[To be written in next phase based on results of Gap Analysis.]

Annex A:
Discussion on TSP and CSP Concept

There has been confusion over the use of the term Certification Service Provider (CSP) within the context of Electronic Signatures and the need to also identify providers of Trust Services not relating to Electronic Signatures. The present document proposes the use of the term Trust Service Provider (TSP) to cover providers of electronic services which enhances trust and confidence in electronic transactions. The term is used in preference to and with a broader application than - the term certification-service-provider (CSP) defined in Directive 1999/93/EC [i.1].

The term "Trust Service Provider", while not restricted to electronic signatures, can encompass, when related to electronic signatures:

- TSPs supporting electronic signatures covering notably, as listed in clause 5.3.5, Trust Service Providers issuing qualified (TSP_{QC}) and/or non-qualified certificates (TSP_{PKC}), time-stamping service providers (TSSPs), signature generation service providers (SGSPs), and signature validation service providers (SVSPs); and

- Trust Application Service Providers (TASPs), i.e. TSP applying electronic signatures for building added value Trust Services on top of electronic signatures. This covers e.g. registered electronic mail (REM) or registered electronic delivery (RED) service providers, and information preservation service providers (IPSPs).

Note that the term CSP as defined in Directive 1999/93/EC [i.1] covers those two categories.

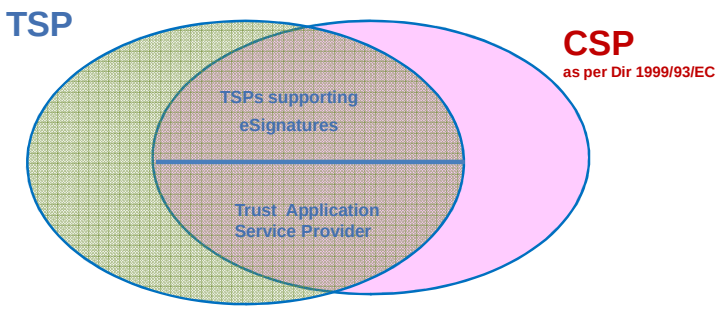


Figure A.1: Illustration of relationship between TSP and CSP

The term CSP as defined in Directive 1999/93/EC is commonly used to cover electronic services to support electronic signatures such as listed in clause 5.3.5.

However, this term CSP can also be used to describe non-electronic services supporting electronic signatures such as providers of consulting services on Electronic Signatures. Also, it is not clear whether services applying electronic signatures, as listed in clause 5.3.6, are also examples of a CSP.

The term TSP is not restricted to TSPs supporting electronic signatures (as addressed in clause 5.3.5) but also includes Trust Application Service Providers (TASP) as listed in clause 5.3.6 as well as trust applications not employing electronic signatures. For example TSP encompasses TSPs providing services for long term preservation using secure storage instead of electronic signatures.

Annex B: Initial Guidance on Matching Business Requirements to Electronic Signature Standards from Signature Creation / Validation Viewpoint

B.1 Introduction

A major new area identified in the Rationalised Framework given in clause 5 is the need for business driven guidance for the selection of the appropriate standards and options. This annex provides some initial proposals for an approach to the business guidance.

B.2 The Guidance Approach

It is recognised that guidance is needed to assist in the selection of standards for electronic signature and their implementation in an electronic business process. In order to assist the stakeholder (users, suppliers, regulators, etc.) once he conducted his analysis on the business requirements for the use for eSignatures, the guidance first identifies eSignature business factors that are important when implementing electronic signatures and commonly should be considered in selecting the appropriate solution. Having identified the business factors applicable to the business context (e.g. through a business analysis), the guidance will assist the stakeholder in mapping the applicable business factors into the selection of the appropriate standards and the technical rules for their implementation (potentially including initialisation and parameter configuration of those standards and their options).

Figure B.1: Phased approach used as Basis for Guidance

Based on this phased approach (requirements analysis, identification of business factors, selection of standards and technical rules for their implementation) illustrated in the above Figure, the guidance documents will provide a tutorial-based guided approach on each step of the last two phases through a list of questions the business stakeholders should address and answer, as well as through best-practice driven tips and guidance.

The basis of this approach is to consider the requirements from the viewpoint of signature creation and validation and work out towards other areas which facilitate the creation and validation of electronic signatures.

Having selected the appropriate standards and options it is recommended that the applicable rules for signature creation and validation are specified in more detail within a Signature Policy covering both technical and wider procedural, data and physical requirements, such as identified in clause 5.2.2 as EN 366 101. The technical aspects of such a policy document requiring to be used to control the operation of a signature creation and validation application may be represented in human readable or electronic form as identified in clause 5.2.2 as EN 366 162.

B.3 Business factors

Back to the Business Analysis part of this phased approach in specifying electronic signature in a business process, when specifically identifying and addressing each and every electronic signature of an electronic business process, a set of signature specific factors will be of particular relevance and need to be selected in the light of the business requirements assessment resulting from the analysis of the associated business, policy and legal requirements.

Those signature specific factors identified here below highlight the fact that the creation and verification process of an electronic signature may rely on the provision of external (trusted) services and functional elements for which an appropriate and rationalised standardisation will ease a reliable, trustworthy and successful implementation.

To ensure the selection of standardised functional areas (as identified in clause 5) matches the needs of the business requirements to be implemented with the help of electronic signatures, the following factors need to be taken into account. In particular they will impact the effective choices and selection of standards for the technical implementation:

- **Factors mainly related to the application for which electronic signature implementation is required:**

NOTE 1: Even if they can also be driven by legal provisions, these factors may be considered as being mainly related to the "application".

a) **The type of data to be signed**: The type of application technology and the format of the Data To Be Signed (e.g. binary, structured data, xml, PDF document, editable documents such as Word or ODF, multimedia packages, images, etc.) may have an impact on the signature format to be used (e.g. CAdES, XAdES, PAdES). The type of format for the DTBS may also be influenced by business risks or legal provisions, for example, when a specific provision is imposed on the formalities of signing (e.g. what you see is what you sign).

b **Workflow requirements** implied by the application (e.g. single signature, multiple serial / parallel signatures) may have an impact on the profiling signature format to be used (e.g. CAdES, XAdES, PAdES).

c) **The relationship between the signed data and the signature**: The type of relationship between the signed data and the need for signed data referencing mechanisms (e.g. signature of document references being hashes of the referenced documents) may have an impact on the way this relationship is implemented (e.g. associated, encapsulated, encapsulating) and the signature format to be used.

d) **Bulk Signing requirements**: Requirements, if any, for bulk signing of a significant number of documents per day may have an impact on, for example, requirements for use of signing devices designed for bulk signing (e.g. Hardware Security Modules).

e) **Timing and sequence**: Requirements for timing or sequencing signed data to provide evidence of the sequence of events can impact on, for example, requirements for time-stamping services and on the form of the considered signature format (e.g. –T, a form that includes a trusted time-stamp that covers and protect the basic signature elements) and provide timing constraints for signature creation and verification procedures.

f) **Community**: The community within which the signatures are to be exchanged whether global, European, national or sector specific. This may influence the need to adopt standards appropriate to that community.

g) **Support for other identity authentication services:** electronic signature services may be required to operate alongside other authentication services, for example providing corporate identity authentication of web related services such as provided by CABForum extended validation services, or electronic identity authentication for authentication of user access to those services. In such cases the supporting user signing / identity devices and Trust Service Providers may be used to provide integrated support for electronic signatures and identity authentication. Harmonisation of standards in these two areas will help to optimise the provision of such services.

- **Factors mainly influenced by legal provisions associated to the business context in which the business process takes place:**

h) **Signature legal level**: The signature legal level required in the context of the business process and the associated legal requirements:

i. ***Qualified level***: for use of signatures recognised as equivalent to handwritten signatures as specified in article 5.1 of the Electronic Signatures Directive [i.1];

ii. ***Advanced level with a Qualified Certificate***: for use of Advanced Electronic Signatures as specified in article 2.2 of the Electronic Signatures Directive [i.1] with the requirements on a high level of assurance with regards to the authentication of the signatory (Comparable with Level of Authentication 4 as defined in ISO CD 29115) and recognised as granted with a non-deniable legal effect as specified in article 5.2 of [i.1];

NOTE 2: This level is explicitly introduced in Commission Decisions CD 2011/130/EU [i.14] establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market.

iii. ***Advanced level***: for use of Advanced Electronic Signatures as specified in article 2.2 of the Electronic Signatures Directive [i.1], and recognised as granted with a non-deniable legal effect as specified in article 5.2 of the Electronic Signatures Directive [i.1];

iv. ***Simple level***: for use of Electronic Signatures as specified in article 2.1 of the Electronic Signatures Directive [i.1], and recognised as granted with a non-deniable legal effect as specified in article 5.2 of the Electronic Signatures Directive [i.1].

NOTE 3: "Simple level" signatures are considered outside the scope of the current ETSI CEN signature standardisation activity.

This factor has an impact on the level of assurance on the authentication (i.e. the certification of the identification) of the actor applying an electronic signature, on the class and policy requirements on the TSP providing such level of assurance, on the class of signature creation device used by such actors, on the use of a specific trust model for TSP issuing certificates (e.g. Trusted Lists, specific Trust Anchors in PKI hierarchy, use of CA certificate stores).

i) **Scope and purpose of the signature**: The statement of the signature scope and purpose and/or the type of commitment associated with the signature.

j) **Formalities of signing**: Requirements related to the formalities of signing may have an impact on the

- requirement for having a WYSIWYS environment;
- requirements for providing the actor applying electronic signatures with:
  - i. proper advice and information on the application's signature process,
  - ii. proper advice and information on legal consequences,
  - iii. a user interface guaranteeing, to the extent possible, a valid legal signature environment.
- requirements for providing the relying party (including the signatory) with correct procedures for the verification and the archival of the electronic signature and the verification data.

This may impact the selection of appropriate protection profiles and conformity assessment schemes against which the signature creation and verification application will be designed and assessed.

k) **Durability**: Requirement for durability of the electronic signature such that it is verifiable after a given period of time, such as:

i. very long term (more than 10 years),

ii. long term (1 to 10 years),

iii. medium term (1 day up to 1 year),

iv. short term (transaction lifetime - less than 1 day).

This can impact on, for example, the type of signature "form" required (e.g. BES, -T or –A or LTV as specified in CAdES, XAdES and PAdES) and associated requirements for time-stamp services, as well as the cryptographic suite employed.

- **Factors related to the actor applying an electronic signature:**

l) The **Type of Actor** applying an electronic signature, such as:

i. physical person,

ii. legal person or organisational entity such as a company or government department, or parts thereof,

iii specific device belonging to an identified legal or physical person,

iv. specific application acting for an identified legal or physical person.

This can impact on, for example, the type of signature creation device required and the policy requirements for the registration aspects of the TSP issuing certificates.

m) The level of assurance required for the **authentication** of the actor applying electronic signature, such as:

i. Level of Assurance 4: very high confidence of authentication required. This LoA shall be used when a high risk is associated with erroneous authentication. (Qualified level) (Comparable with LoA 4 as defined in ISO CD 29115.)

ii. Level of Assurance 3: high confidence required in an asserted identity. This LoA shall be used where substantial risk is associated with erroneous authentication. (Advanced level) (Comparable with LoA 3 as defined in ISO CD 29115.)

NOTE 4: Requirements comparable with ISO CD 29115 LoA 2 and 1 are considered outside the scope of the current ETSI CEN signature standardisation activity.

NOTE 5: Additional requirements may be stated on "revocation support" for related authentication credentials/tokens, or statement on the trust model required for the TSP issuing certificates (e.g. specific (set of) trust anchor(s), specific (set of) certificate policy OID(s)).

NOTE 6: Additional requirements may be defined with regards to the level of assurance on roles and other identity attributes that may be associated to the bare identity of the actor applying electronic signature, whatever type of actor it is. In other words, the identification data covered by such required level of assurance with regards to the authentication of the actor applying electronic signature may consist of a set of identity attributes more complex than its "basic" identity. This can impact on, for example, the level of TSP service required and the level of signature creation device employed (e.g. an SSCD may not be desirable, in particular, when an $AdES_{QC}$ and not a QES is required), the Certificate Validity Status services, on the use of additional signature attributes that will be added to the DTBS when creating the signature and hence have an impact on the implementation of the selected signature format.

n) Requirement for (Actor's) **Signature Creation Devices**:

i. According classification of signature creation devices to be defined. A suggested 4 level system is from the highest level (L4) covering the requirements for SSCD, L3, L2 and L1.

ii. Potential signing support with simple user devices, such as mobile phones, which do have limited processing and interfacing capabilities.

NOTE 7: Such requirements may be clearly expressed in terms of business needs as from business risk mitigation, budgetary impact, or legal requirements.

This can impact on, for example, requirements for signing devices and potentially use of TSPs supporting document signing.

- **Other signature parameters:**

o) Requirements for other information to be associated with the signature such as:

i. Location at which the signature takes place,

ii. The time of signing.

This may have an impact on the use of additional signature attributes that will be added to the DTBS when creating the signature and hence an impact on the implementation of the selected signature format

p) **Robustness of Signature Cryptographic Suites**: Requirements on Signature cryptographic suites (e.g. setting any of the parameters may be forced by legal requirements or a specific policy).

q) **Responsibility on Verifier**: This may cover the expression of the enforcement of specific requirements on the verifier of the electronic signatures (e.g. endorse and apply verification requirements as expressed in a specific policy document, often called a signature policy, the need for extending a basic from a generated signature for reasons dictated by the fact that minimal impact is searched on signatories while verification side has more computational capacities). This may have an impact of the electronic signature form at creation time (e.g. EPES), and on the signature verification procedures.

It is worth stressing again that the configuration of the above described eSignature Business Factors will in practice be determined by the careful analysis of:

a) The business context requirements, including but not limited to

   i. The business application domain and its underlying technology

   ii. The business process

   iii. Identified business risks

   iv. The budgetary constraints

e) The associated organisational or application or other security policies applicable

f) The associated legal requirements

g) The mitigation measures resulting from a risk assessment

Annex C: Inventory

TEMPORARY NOTE: The inventory is currently held in a separate document which may be downloaded from the same location where this document is held.

History

Document history		
V0.0.1	July 2011	Pre-processed by the ETSI Secretariat ***editHelp!*** E-mail: mailto:edithelp@etsi.org
V0.0.2	Aug 2011	Draft for Public review