ETSI SR 001 604 V1.1.1 (2012-07)

Rationalised Framework for Electronic Signature Standardisation

Reference
DSR/ESI-000099

Keywords
e-commerce, electronic signature, security

CEN

Avenue Marnix 17
B-1000 Brussels - BELGIUM

Tel: + 32 2 550 08 11
Fax: + 32 2 550 08 19

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

Contents

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 [i.1].

Emerging cross-border use of eSignatures and the increasing use of several market instruments (e.g. Services Directive [i.3], Public Procurement [i.4] and [i.5], eInvoicing [i.6]) 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.7] 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.8] 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.9], consequently issued by the Commission to CEN, CENELEC and ETSI for updating the existing eSignature standardisation deliverables, CEN and ETSI have set up the eSignature Coordination Group in order to coordinate the activities achieved for Mandate 460. One of the first tasks in 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. The following web site was set up in the framework in Mandate 460: http://www.e-signatures-standards.eu/.

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) An inventory of existing electronic signature standardisation.

b) A target rationalised structure for future European eSignatures standardisation documents.

c) The results of an existing versus target 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.

[i.5] 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.6] Council Directive 2006/112/EC of 28.11.06 on the common system of value added tax.

[i.7] "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.8] "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.9] 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.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 3", July 2009.

[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.1254/ISO/IEC DIS 29115: "Information technology - Security techniques - Entity authentication assurance framework".

NOTE: A further inventory of documents relating to electronic signature is given in annex D.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions taken from Directive 1999/93/EC [i.1] apply:

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 certificates" for designating the Trust Service Provider who issues certificates and provides related certificate creation, assignment and life cycle management services.

certificate validation: process of checking that a certificate or certificate path is valid

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].

secure signature creation device: signature creation device which meets the requirements laid down in Annex III 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

signature validation: process of checking that a signature is valid including overall checks of the signature against local or shared signature policy requirements as well as certificate validation and signature (cryptographic) verification

signature verification: process of checking the cryptographic value of a signature using signature verification data

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:

Data Preservation Service Provider (DPSP): Trust Application Service Provider which provides Trust Services to which data, 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

NOTE: This service is expected to be able to exhibit all preserved data 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.

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

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

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: list of the trust service status information, protected to assure its authenticity and integrity, from which interested parties may determine whether a trust service has been assessed as operating in conformity with recognised criteria for a given class of trust service

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: profile of the trust service status list that is the 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 [i.1]

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
ANSSI	(French) Agence national de la Sécurité de Systèmes d'Information
API	Application Program Interface
ASiC	Associated Signature Containers
BES	Basic Electronic Signature (used with CAdES/XAdES and PAdES)
BSI	Bundesamt für Sichereit (German Federal Office for Information Security)
CA	Certification Authority
CAB Forum	CA Browser Forum
CAdES	CMS Advanced Electronic Signature
CD	[European] Commision Decision
CEN	Comité Européen de Normalisation
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
CSP	Certification Service Provider
CWA	CEN Workshop Agreement
DIS	Draft International Standard
DPS	Data Preservation System
DPSP	Data Preservation Service Provider
DSS	Digital Signature Standard (as published by OASIS)
E-CODEX	e-Justice Communication via Online Data Exchange
EESSI	European Electronic Signature Standardization Initiative
EN	European Norm
EPES	Explicit Policy Electronic Signature (used with CAdES / XAdES and PAdES)
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IAS	Identification, Authentication and Digital Signature
IDPF	International Digital Publishing Forum
ISO	International Organization for Standardization
LoA	Level of Assurance

NOTE: As specified in [i.21].

LTV	Long term Validation (used with PAdES)
MTM	Mobile Trusted Module
NFC	Near Field Communication
OCSP	Online Certificate Status Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OEBPS	Open E-Book Publishing Structure
PAdES	PDF Advanced Electronic Signature
PKC	Public Key Certificate
PEPPOL	Pan-European Public eProcurement On-Line
PP	Protection Profile
QC	Qualified Certificate
QES	Qualified Electronic Signature
RED	Registered Electronic Delivery
REM	Registered Electronic Mail
REM-MD	Registered Electronic Mail – Management Domain
SCA	Signature Creation Application
SGSP	Signature Generation Service Provider
SOGIS	Senior Officials Group – Information Systems Security
SP	Signature Policy
SR	Special Report
SCD	Signature Creation Device
SSCD	Secure Signature Creation Device
SMIME	Secure Multi-Purpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol

SOAP	Simple Object Access Protocol
SPOCS	Simple Procedures Online for Cross-border Services
STORK	Secure identity across borders linked) being the most relevant
SSL	Secure Socket Layer
SVA	Signature Validation Application
SVSP	Signature Validation Service Provider
TASP	Trust Application Service Provider
TC	Technical Committee
TOE	Target of Evaluation
TEE	Trusted Execution Environment
TL	Trusted List
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
UPU	Universal Postal Union
USB	Universal Serial Bus
WI	Work Item
XAdES	XML Advanced Electronic Signature
XSL	eXtensible Stylesheet Language
XML	eXtensible Markup Language

NOTE: See: http://encyclopedia2.thefreedictionary.com/Extensible+Markup+Language

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 as an Excel spreadsheet form and a PDF form that are 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 structure

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 approach, with guidance on the use of standards in business terms, 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 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 [i.1] 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 providers 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, who are stakeholders willing to introduce and implement eSignatures in a business electronic process, the rationalised structure will provide a viewpoint 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 whether 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, whether business or governmental entities, providing trusted services, the rationalised structure will provide additional targeted guidance from the viewpoint of the trust service provider. This guidance will focus on the selection of standards relevant to particular trust services. Guidance will be provided not only for trust service providers supporting electronic signatures (e.g. trust service providers issuing qualified certificates) but also for those trust application providers using electronic signatures (e.g. registered electronic mail).

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 also aims 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 structure has been organised around 6 (functional) areas and 5 types of documentation.

NOTE: Clause 5.2.5 discusses how this classification scheme may be expanded to support standardisation for Identification, Authentication and Signatures currently being investigated in a review of the Electronic Signatures Directive.

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, according to Common Criteria i.17 for signature creation/verification applications.

2) **Signature Creation and Other Related Devices:** This area will focus on standards related to Secure Signature Creation Devices as defined in the Signature Directive, on signature creation devices used by Trust Service Providers as well as other types of devices supporting electronic signatures and related services such as authentication.

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 algorithms, 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, including web server certificates, Time-Stamping Services Providers, TSPs offering signature validation services, TSPs offering remote signature creation services (also called signing servers). The current list covers those services supporting electronic signature which exist to date; other Trust Services may be identified at a future date.

NOTE: The term "Trust Service Provider supporting eSignature" 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/validation of electronic signatures in normal operation. This includes namely registered mail and other e-delivery services, as well as data preservation (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.

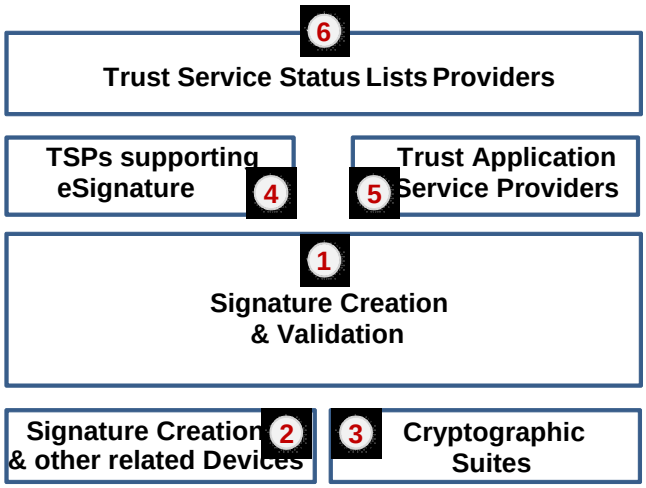


Figure 1: Overview of the Rationalised structure for electronic signature standardisation

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. The arrows indicate where business decisions made in one area may have influence in business decisions in another area.

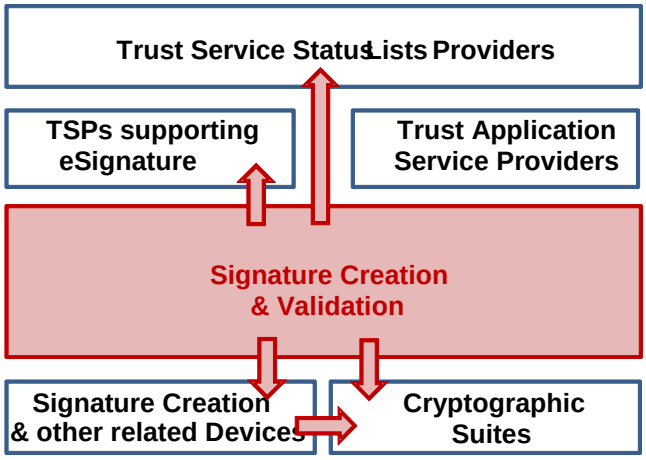


Figure 2: Signature Creation & validation viewpoint of Rationalised structure

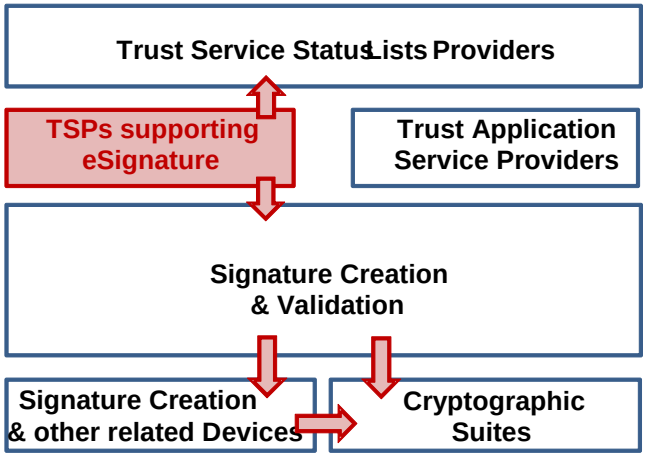


Figure 3: TSPs supporting eSignatures viewpoint of Rationalised structure

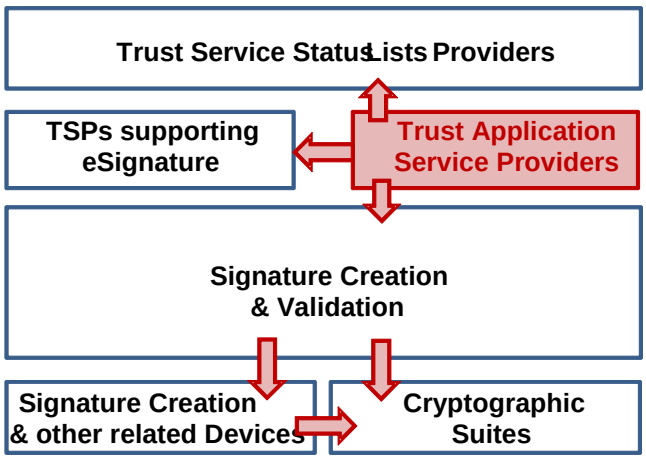


Figure 4: Trust Application Service Providers viewpoint of Rationalised structure

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 provides 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, etc.

4) **Conformity Assessment:** This type of document addresses requirements for assessing the conformity of a system claiming conformity to a specific set of technical specifications, policy or security requirements (including protection profiles when applicable). This primarily includes conformity 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 tests or testing systems that will provide automated checks of compliance of products, services or systems with specific set(s) of technical specifications.

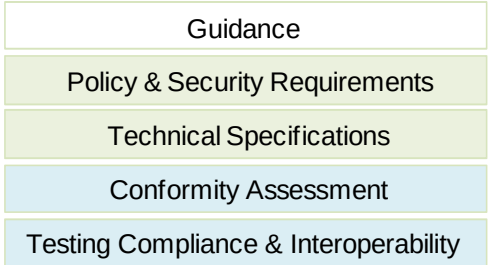


Figure 5: Illustration of Document Types in the Rationalised structure

5.2.3 Rationalised structure with Sub-Areas

This rationalisation of the structure for eSignature standardisation framework for some area can be broken down into further sub-areas as illustrated in figure 6. 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.

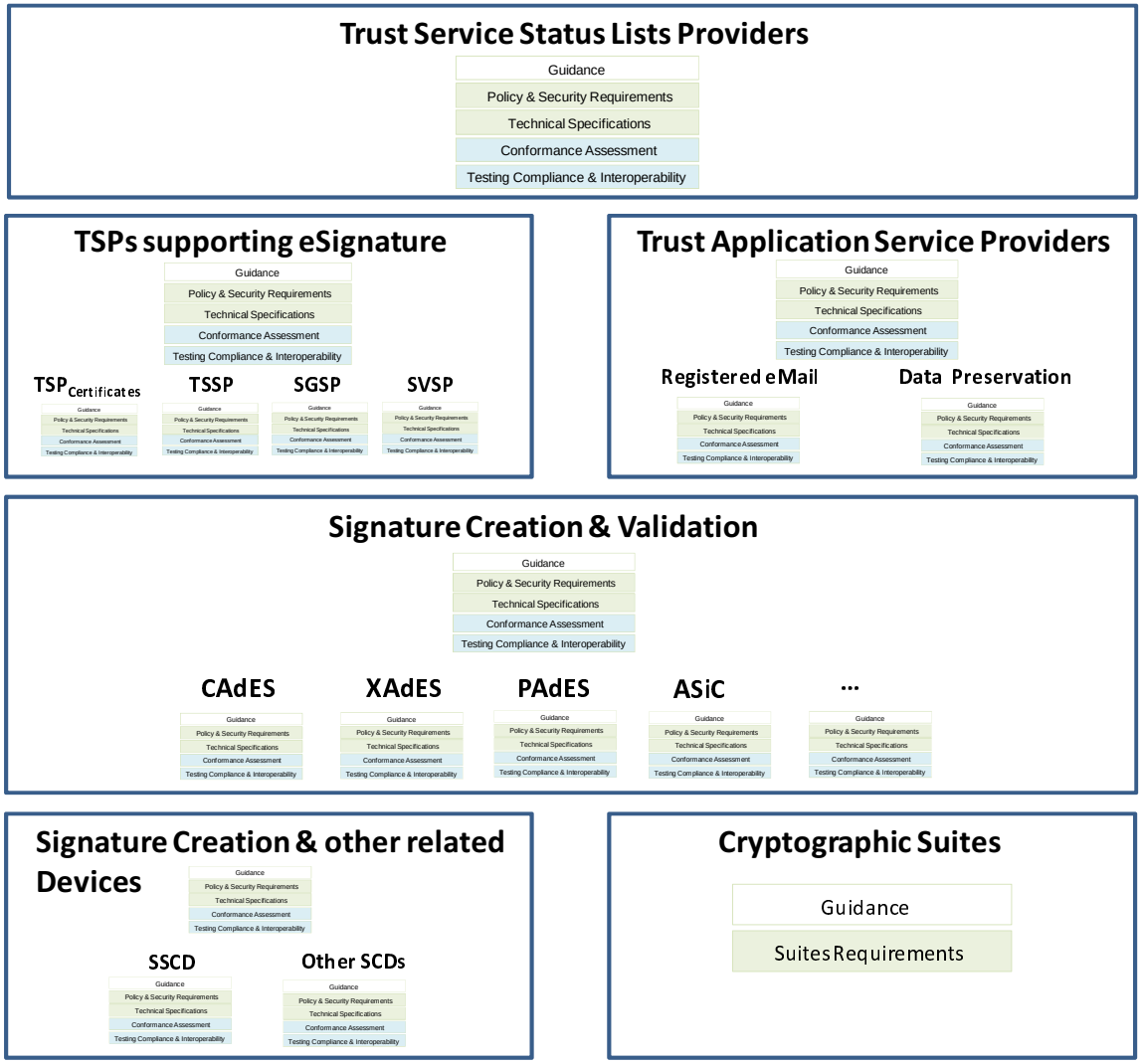
So far sub-areas have been identified in areas 1, 2, 4 and 5.

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. Advanced Electronic Signatures in Mobile environments are also considered as part of this area.

In area 2, Signature Creation Devices, two sub-areas have been identified to group documents with regards to the type of signature creation device, namely Secure Signature Creation Devices (SSCDs) 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 certificates, 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) services provisioning, and the one dedicated to Data Preservation Service Providers (DPSP).



NOTE: Boxes below titles in figure, listing document types, have all the same content as the one displayed in top area except for bottom right area.

Figure 6: Illustration of Rationalised structure with Sub-areas

5.2.4 Numbering Scheme

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

DD L19 xxx-z

Where:

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

L when set to 4: identifies a CEN deliverable

when set to 0, 1, 2, or 3: identifies an ETSI deliverable and the type of deliverable in the standardisation process

019 for ETSI published Special Reports (SR)
119 for ETSI published Technical Specification (TS) and Technical Report (TR)
219 for ETSI published Standard (ES) and ETSI Guide (EG)
319 for ETSI published European Norm (EN)

419 for CEN published Technical Specification (TS) or European Norm (EN)

NOTE 1: The present document omits this L digit.

19 indicates the series of standardisation documents related to eSignatures

ETSI/CEN may further extend this numbering system in line with their own practices.

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-Conformity Assessment; 4- Testing Compliance and Interoperability)).

-z identifies multi-parts as some documents may be multi-part documents.

Additional numbering for identifying parts and versions will be in line with ETSI or CEN conventions depending on which organisation publishes the document.

NOTE 2: Annex C outlines the proposed migration strategy from the current number allocation to the new numbering.

5.2.5 Possible Extension of Classification Scheme to incorporate Identification, Authentication and Signature Standards

The European Commission has indicated its possible intention to revise the electronic signature Directive 1999/93/EC [i.1] to include electronic Identification, Authentication and Signatures policy provisions. A short consideration of a possible extension to the classification suggests that this can be incorporated in the rationalised structure with the necessary extension of scopes. This may involve, for example:

a) An additional area created to cover systems requiring to provide, update and verify credentials and other trust tokens for electronic identification and authentication.

b) Extensions to standardisation within existing areas with modified scope as needed to support identification, authentication and signatures (e.g. trust service providers, secure devices, cryptographic suites, trust status lists providers).

c) Further additional areas as needed for Identification, Authentication and Signatures.

The classification of document types described in clause 5.2.3 is considered to be equally applicable to Identification, Authentication and Signatures aspects.

It is planned to consider this further in the next phase and take into account emerging technologies in Identification, Authentication and Signatures.

5.3 Rationalised structure by Area

5.3.1 Generic

The generic document for electronic signatures standardisation includes:

TR 19 000 Rationalised structure for Electronic Signature Standardisation

This document is to provide the framework for the 19 000 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 validation (TR 19 100) 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. It will include a basic classification on assurance levels to be used across all the areas. In addition, this will establish definition of commonly applicable terms.

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	19	1	0	0	Business Driven Guidance for Signature Creation and Validation
				Policy & Security Requirements	
EN	19	1	0	1	Policy & Security Requirements for Signature Creation and Validation
EN	19	1	1	1	Protection Profiles for Signature Creation and Validation Application
				Technical Specifications	
EN	19	1	0	2	Procedures for Signature Creation and Validation
EN	19	1	2	2	CAdES - CMS Advanced Electronic Signatures
EN	19	1	3	2	XAdES - XML Advanced Electronic Signatures
EN	19	1	4	2	PAdES - PDF Advanced Electronic Signatures
EN	19	1	5	2	Advanced Electronic Signatures in Mobile environments
EN	19	1	6	2	ASiC - Associated Signature Containers
EN	19	1	7	2	Signature Policies
				Conformity Assessment	
EN	19	1	0	3	Conformity Assessment for Signature Creation & Validation Applications (& Procedures)
				Testing Compliance & Interoperability	
TS	19	1	0	4	General requirements on Testing Compliance & Interoperability of SC&V
TS	19	1	2	4	CAdES Testing Compliance & Interoperability
TS	19	1	3	4	XAdES Testing Compliance & Interoperability
TS	19	1	4	4	PAdES Testing Compliance & Interoperability
TS	19	1	5	4	Testing Compliance & Interoperability of AdES in Mobile environments
TS	19	1	6	4	ASiC Testing Compliance & Interoperability
TS	19	1	7	4	Testing Compliance & Interoperability of Signature Policies

Guidance

TR 19 100 Business Driven Guidance for Signature Creation and Validation

This document provides business guidance for the use of electronic signature standards from the viewpoint of signature creation and validation. As clause 5.2.1, figure 2 illustrates, business decisions made in this area influence business decisions made in almost the rest of the areas of the Rationalized Framework. This will include guidance on selection between the different signature formats. Further information on the proposed approach to such business guidance is given in annex B.

Policy and Security Requirements

EN 19 101 Policy and Security Requirements for Electronic Signature Creation and Validation

This document provides policy and security 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 19 172). This includes requirements for the secure operation of signature creation and validation applications such as might be provided by an information security management system.

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: 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].

EN 19 111 Protection Profiles for Signature Creation & Validation Applications

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

- **Introduction:** this document is an introduction that defines the security requirements for Signature Creation Applications (SCA) and Signature Validation Applications (SVA). It defines terms used in all parts, the SCA/SVA, their functions, and their environment.
- **Core PP for an Signature Creation Application:** this document specifies a protection profile for an SCA. It defines security requirements for SCA conformity from the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this Protection Profile (PP) corresponds to software, running on an operating system and hardware, the Signature Creation Platform. The TOE, using services provided by the Signature Creation Platform and by an SSCD allows the signatory to generate an electronic signature.
- **Extensions to Core PP for an SCA.**
- **Core PP for an SVA:** this document specifies a protection profile for an SVA. It defines security requirements for SVA conformity from the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to software, running on an operating system and hardware, the Signature Validation Platform. The TOE, using services provided by the Signature Validation Platform and by the environment allows the verifier to check an electronic signature.
- **Extensions to Core PP for an SVA.**

Technical Specifications

EN 19 102 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), PAdES (PDF Advanced electronic signature), AdES in Mobile environments and ASiC (Associated Signature Containers) signatures taking into account use of Trust Lists.

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

- **Signature creation.**
- **Signature validation.**

EN 19 122 CMS Advanced Electronic Signatures (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:

- **Overview of CAdES** and its profiles, and the relationship between them.
- **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 minimum set of options that are appropriate for maximizing interoperability between CAdES signatures.

NOTE 1: The baseline profile defines a baseline profile for CAdES that provides the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of AdES signatures to be interchanged across borders. In particular it takes into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the European Services Directive [i.15].

- **CAdES eInvoicing Profile:** This document specifies a profile identifying a common set of options for eInvoicing, building on the baseline.

NOTE 2: Additional community specific profiles might be required for other communities.

EN 19 132 XML Advanced Electronic Signatures (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:

- **Overview of XAdES** and its profiles, and the relationship between them.
- **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 1: 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.

NOTE 2: The baseline profile defines a baseline profile for XAdES that provides the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of AdES signatures to be interchanged across borders. In particular it takes into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the European Services Directive [i.15].

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

NOTE 3: Additional community specific profiles might be required for other communities.

EN 19 142 PDF Advanced Electronic Signatures (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 [**i.13**]:** This document profiles the use of PDF signatures, based on CMS, as described in ISO 32000-1 [i.13], 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 [i.13] 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 19 122.

- **PAdES Long Term - PAdES-LTV Profile:** This document profiles the electronic signature formats found in ISO 32000-1 [i.13] 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 19 122 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 19 132, for signing XML content within the PDF containers, including the following situations:

  - One XML document (compliant with an arbitrary XML language, like Universal Business Language 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 XML Forms Architecture 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 validation representation: The visual representation of the validation 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.

NOTE 1: The baseline profile defines a baseline profile for PAdES that provides the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of AdES signatures to be interchanged across borders. In particular it takes into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the EU Services Directive [i.15].

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

NOTE 2: Additional community specific profiles might be required for other communities.

EN 19 152 Advanced Electronic Signatures in Mobile Environments

This document will provide details on the framework (including architecture and relevant scenarios) required for the creation and validation of advanced electronic signatures in the mobile environment (Advanced Electronic Signatures in Mobile Environments). Part of the specifications required for implementing the aforementioned framework may be defined within this document. Other may be included by reference to other external documents.

EN 19 162 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 base specification and associated profiles.

This multi-part document includes:

- **Overview of ASiC** and its profiles, and the relationship between them.
- **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 19 122, XAdES detached signature(s) as specified in EN 19 132; 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.

NOTE 1: The baseline profile defines a baseline profile for ASiC that provides the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications to be applicable to a wide range of communities when there is a clear need for interoperability of AdES signatures, on which ASiC is based, to be interchanged across borders. In particular it takes into account needs for interoperability of AdES signatures used in electronic documents issued by competent authorities to be interchanged across borders in the context of the European Services Directive [i.15].

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

NOTE 2: Additional community specific profiles might be required for other communities.

EN 19 172 Signature Policies

This document 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:

- **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 and other signature policy formats.
- **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 signing 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 validation of electronic signatures.
- **ASN.1 format for Signature Policies:** This document specifies an ASN.1 format for those parts of the Signature Policy that may be structured and are worth to be automatically processed by both signing 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 validation of electronic signatures.

Conformity Assessment

EN 19 103 Conformity 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 conformity rules for assessing conformity of SCA or SVA against Policy Requirements. This will show the complete process for performing complete assessment and make some reference to other conformity assessment guidance (including technical specifications, protection profiles, signature policies.

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

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

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

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

Testing Compliance & Interoperability

TS 19 104 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 19**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 19 124 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 conformity assessment for signature creation and validation applications (EN 19 103) 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 multi-part document covering the following topics:

- **Test suites for testing interoperability of CAdES signatures:** This document would be used by 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 19 122.

- **Test suites for testing interoperability of Baseline CAdES signatures:** This document would be used by 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 19 122.

- **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 will allow developing a tool that can automatically check that a CAdES signature is fully compliant with the relevant aforementioned specifications, without claiming any statement on its validity.

- **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 will allow developing a tool that can automatically check that a CAdES Baseline signature is fully compliant with the relevant aforementioned specifications, without any statement on its validity.

- **Specifications for testing compliance of CAdES Signatures validation:** This will allow developing a tool that can automatically check that a generated CAdES signature is fully compliant with the relevant aforementioned specifications and validate the signature according to EN 19 102.

NOTE 1: A study should be made for assessing the need of a separate part for supporting compliance testing of signature validation.

NOTE 2: A study should be made for assessing the need of an additional part for supporting the potential development and/or maintenance of a reference implementation.

TS 19 134 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 conformity assessment for signature creation and validation applications (EN 19 103) 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 multi-part document structured as follows:

- **Test suites for testing interoperability of XAdES signatures:** This document will be used by 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 19 132.

- **Test suites for testing interoperability of Baseline XAdES signatures:** This document will be used by 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 19 132.

- **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 will allow developing a tool that can 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 will allow developing a tool that can automatically check that a XAdES Baseline signature is fully compliant with the relevant aforementioned specifications, without claiming any statement on its validity.

- **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 19 102.

NOTE 1: A study should be made for assessing the need of a separate part for supporting compliance testing of signature validation.

NOTE 2: A study should be made for assessing the need of an additional part for supporting the potential development and/or maintenance of a reference implementation.

TS 19 144 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 conformity assessment for signature creation and validation applications (EN 19 103) 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 multi-part document structured as follows:

- **Overview.**
- **Test suites for testing interoperability of PAdES signatures:** This document will be used by 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 19 142.
- **Test suites for testing interoperability of Baseline PAdES signatures:** This document will be used by 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 19 142.
- **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 will allow developing a tool that can 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 will allow developing a tool that could automatically check that a PAdES Baseline signature is 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 will allow developing a tool that can automatically check that a PAdES signature is fully compliant with the relevant aforementioned specifications and validates the signature according to EN 19 102.

NOTE 1: A study should be made for assessing the need of a separate part for supporting compliance testing of signature validation.

NOTE 2: A study should be made for assessing the need of an additional part for supporting the potential development and/or maintenance of a reference implementation.

TS 19 154 Testing Compliance & Interoperability of AdES in Mobile environments

This document provides technical specifications for helping implementers and accelerating the development of creation and validation applications for advanced electronic signatures in mobile environments.

TS 19 164 ASiC 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 conformity assessment for signature creation and validation applications (EN 19 103) with policies requiring conformity to ASiC formats and procedures. First, it will define test suites as complete as possible for supporting the organization of interoperability testing events where different ASiC related applications may check their actual interoperability. Additionally, it will include the specifications required for building software tools for actually testing technical compliance of ASiC against the relevant ASiC related technical specifications.

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

- **Overview.**
- **Test suites for testing interoperability of ASiC:** This document will be used by entities interested in testing tools that generate and verify ASiC not adhered to any specific profile, but compliant with the mother ASiC specification as defined in EN 19 162.
- **Test suites for testing interoperability of Baseline ASiC:** This document will be used by entities interested in testing tools that generate and verify ASiC that claim to be compliant with the ASiC Baseline Profile as specified in EN 19 162.
- **Specifications for testing compliance of ASiC:** This document will specify, among other things, rules for testing compliance of signatures against the ASiC specification. It will allow developing a tool that can automatically check that generated ASiC are fully compliant with the relevant aforementioned specifications, without any statement on their validity.

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

- **Specifications for testing compliance of ASiC validation:** This will allow developing a tool that can automatically check that ASiC are fully compliant with the relevant aforementioned specifications and that validates the signature according to EN 19 102.

NOTE 1: A study should be made for assessing the need of a separate part for supporting compliance testing of signature validation.

NOTE 2: A study should be made for assessing the need of an additional part for supporting the potential development and/or maintenance of a reference implementation.

EN 19 174 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 conformity assessment for signature creation and validation applications (EN 19 103) with policies requiring conformity to machine processable Signature Polices format specifications.

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

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

5.3.3 Signature Creation and Other Related 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 and Other Related Devices

		Signature creation and other related devices				
		Sub-areas				
			Guidance			
TR	19	2	0	0	Business Driven Guidance for Signature Creation and Other Related Devices	
			Policy & Security Requirements			
EN	19	2	1	1	Protection Profiles for Secure Signature Creation Devices	
EN	19	2	2	1	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures	
EN	19	2	3	1	Security requirements for trustworthy systems supporting time-stamping	
EN	19	2	4	1	Security Requirements for Trustworthy Systems supporting Server Signing (Signature Generation services)	
EN	19	2	5	1	Protection Profiles for Authentication Device	
			Technical Specifications			
EN	19	2	1	2	Application Interfaces for Secure Signature Creation Devices	
			Conformity Assessment			
EN	19	2	0	3	Conformity Assessment of Secure Devices and Trustworthy systems	
			Testing Compliance & Interoperability			
-	-	-	-	-	*no requirement identified*	

Guidance

TR 19 200 Business Driven Guidance for Signature Creation and Other Related Devices

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

Policy & Security Requirements

Policy and Security Requirements for Signature Creation Devices

No requirement has been identified for this type of document as requirements for the use of signature creation devices is addressed as part of the policy requirements of the signing environment in EN 19 101.

EN 19 211 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.

Additional protection profiles or other form of security certification and security evaluation processes may be required, to ensure that they offer the relevant level of security, for other types of devices such as, e.g.:

- Mobile phones with hardware-based security (TEE, MTM, etc.).
- HSM being recognised as an SSCD.
- SSCD used for mass signing operations (e.g. for signing a series of documents).

EN 19 221 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

This multi-part document specifies security requirements for devices used by Trust Service Providers managing certificates for electronic signatures.

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

- System Security Requirements.

- Protection profile for Cryptographic module for CSP 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 validation of Advanced Electronic Signatures, including, but not limited to, signing qualified certificates, certificate status information, or time-stamp tokens.

- Protection profile for Cryptographic module for CSP 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 validation of Advanced Electronic Signatures e.g. in qualified certificates, certificate status information or time-stamp tokens.

- Protection profile for Cryptographic module for CSP 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.

EN 19 231 Security requirements for trustworthy systems supporting time-stamping

This document defines security requirements for a time-stamping system which consists of at least a time-stamping unit (a set of hardware including an internal clock and software creating time-stamp tokens) and of administration and auditing used to provide time-stamping services.

Informative annexes will provide check lists for conformity assessment.

EN 19 241 Security requirements for trustworthy systems supporting Server Signing (Signature Generation services)

This document specifies security requirements and recommendations for Trustworthy Systems TWSs) supporting server signing. The document is intended for use by developers and evaluators of a Server Signing Application and of its components.

EN 19 251 Protection Profiles for Authentication Device

This multi-part document defines security requirements for conformity of an authentication hardware device (such as, for example, a smart card or USB token) from the perspective of a security evaluation.

This multi-part document covers the following aspects:

- Part1 defines a PP for a device with only the core features and key import. It is the minimum product.

- Part2 defines a PP for a device with key import, key generation, trusted channel with the CA, trusted channel with the Administration application and administration.

- Part3 defines additional features that can be added to part 1 or part2 in order to define a new PP with enhanced features.

Technical specifications

EN 19 212 Application Interfaces 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:

- **Part 1: Introduction.**

- **Part 2** describes **Basic services for electronic signatures:** This document specifies mandatory mechanisms for cryptographic devices such as smart cards, hardware security modules to be used as SSCD, and covers user validation, signature creation, device authentication, password-based mechanisms, establishment of a secure channel and key generation.

- **Part 3** describes **Additional services in the context of electronic signatures:** This document 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 cryptographic verification, identity management and privacy mechanisms.
- **Part 4** describes **Context specific authentication protocols for SSCDs:** This document specifies context specific authentication protocols for SSCDs, covering first the migration to suitable Authentication Protocols, e.g. for further context specific use for other transport layers e.g. NFC, and second a glossary including the unambiguous definition of the security properties employed by the proposed protocols.

Conformity Assessment

EN 19 203 Conformity Assessment of Secure Devices and Trustworthy systems

This document provides guidance on conformity assessment of Secure Creation Devices against the specifications EN 19 211 and guidance on conformity assessment for trustworthy systems against the specifications EN 19 221, EN 19 231, EN 19 241 and EN 19 251.The guidance is intended for use by designated bodies, assessors, evaluators and manufacturers.

Technical Compliance & Interoperability Testing

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	19	3	0	0	Business Driven Guidance for Cryptographic Suites
				Technical Specifications	
TS	19	3	1	2	Cryptographic Suites for Secure Electronic Signatures
				Testing Compliance & Interoperability	
-	-	-	-	-	*no requirement identified*

Guidance

TR 19 300 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 19 312 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

No requirements identified so far.

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	19	4	0	0	Business Driven Guidance for TSPs Supporting Electronic Signatures
				Policy & Security Requirements	
EN	19	4	0	1	General Policy Requirements for TSPs Supporting Electronic Signatures
EN	19	4	1	1	Policy & Security Requirements for TSPs Issuing Certificates
EN	19	4	2	1	Policy & Security Requirements for TSPs providing Time-Stamping Services
EN	19	4	3	1	Policy & Security Requirements for TSPs providing Signature Generation Services
EN	19	4	4	1	Policy & Security Requirements for TSPs providing Signature Validation Services
				Technical Specifications	
EN	19	4	1	2	Profiles for TSPs issuing Certificates
EN	19	4	2	2	Profiles for TSPs providing Time-Stamping services
EN	19	4	3	2	Profiles for TSPs providing Signature Generation Services
EN	19	4	4	2	Profiles for TSPs providing Signature Validation Services
				Conformity Assessment	
EN	19	4	0	3	General requirements and guidance for Conformity Assessment of TSPs supporting e-Signatures
EN	19	4	1	3	Conformity Assessment for TSPs Issuing Certificates
EN	19	4	2	3	Conformity Assessment for TSP providing time-stamping services
EN	19	4	3	3	Conformity Assessment for TSPs providing Signature Generation Services
EN	19	4	4	3	Conformity Assessment for TSPs providing Signature Validation Services
				Testing Compliance & Interoperability	
-	-	-	-	-	*no requirement identified for such a document*

Guidance

TS 19 400 Business Driven Guidance for TSPs Supporting Electronic Signatures

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

NOTE: 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 19 410, 19 420, 19 430, etc. documents for such purpose.

Policy & Security Requirements

EN 19 401 General Policy Requirements for TSPs Supporting Electronic Signatures

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

EN 19 411 Policy & Security Requirements for TSPs Issuing Certificates

This (multi-part) document specifies policy and security requirements for TSPs issuing certificates. It references EN 19 401 for generic requirements.

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

- Overview: This part provides an overview of the other parts of this document. It also describes the relationship of the policy requirements defined in this area and the use of secure devices and trustworthy systems defined in the "Signature Creation and Other Related Device" area.
- Policy requirements for TSP issuing QCs.
- Policy requirements for TSP issuing public key certificates (other than qualified certificates).
- Policy requirements for TSP issuing SSL Extended Validation certificates.
- Policy requirements for TSP issuing SSL baseline certificates.
- Policy requirements for TSP issuing Attribute Certificates:
    - Informative annexes will provide check lists for conformity assessment.

EN 19 421 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 19 401 for generic requirements.

Similarly to EN 19 411, this multi-part document may be organised to include the following topics:

- Overview This part provides an overview of the other parts of this document. It also describes the relationship of the policy requirements defined in this area and the use of secure devices and trustworthy systems defined in the "Signature Creation and Other Related Device" area.
- Policy requirements for TSPs providing Time-stamping services:
    - Informative annexes will provide check lists for conformity assessment.

EN 19 431 Policy & Security Requirements for TSPs providing Signature Generation Services

This document specifies policy requirements for TSPs providing signature generation services. It references EN 19 401 for generic requirements.

Similarly to EN 19 411, this multi-part document may be organised to include the following topics:

- Overview This part provides an overview of the other parts of this document. It also describes the relationship of the policy requirements defined in this area and the use of secure devices and trustworthy systems defined in the "Signature Creation and Other Related Device" area.
- Policy requirements for TSPs providing Signature Generation services:
    - Informative annexes will provide check lists for conformity assessment.

EN 19 441 Policy & Security Requirements for TSPs providing Signature Validation Services

This document specifies policy requirements for TSPs providing Signature Validation Services. It references EN 19 401 for generic requirements.

Similarly to EN 19 411, this multi-part document may be organised to include the following topics:

- Overview: This part provides an overview of the other parts of this document. It also describes the relationship of the policy requirements defined in this area and the use of secure devices and trustworthy systems defined in the "Signature Creation and Other Related Device" area.
- Policy & Security requirements for TSPs providing Signature Validation services:
    - Informative annexes will provide check lists for conformity assessment.

Technical Specifications

EN 19 412 Profiles for TSPs issuing Certificates

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

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

- Overview.
- Certificate profile for certificates issued to natural persons (based on TS 102 280).
- Certificate profile for certificates issued to legal persons.
- Profiles for SSL/TSL Certificates issued to organisation (Baseline and Extended Validation).
- Extensions for Qualified Certificate Profile (based on pre-EN 301 862).

EN 19 422 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 19 432 Profiles for TSPs providing Signature Generation Services

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

EN 19 442 Profiles for TSPs providing Signature Validation Services

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

Conformity Assessment

EN 19 403 General requirements and guidance for Conformity Assessment of TSPs Supporting Electronic Signatures

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

EN 19 413 Conformity Assessment for TSPs Issuing Certificates

This (multi-part) document specifies requirements and provides guidance for the supervision and assessment of a TSP issuing certificates.

NOTE: 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.

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

- Conformity Assessment for Policy Requirements for TSP issuing Certificates.

EN 19 423 Conformity 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.

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

- Conformity Assessment for Policy Requirements for TSP providing time-stamping services

EN 19 433 Conformity 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.

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

- Conformity Assessment for Policy Requirements for TSP providing Signature Generation Services.

EN 19 443 Conformity 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.

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

- Conformity Assessment for Policy Requirements for TSP providing Signature Validation Services.

Testing Compliance & Interoperability

Not applicable so far.

NOTE: At the current date, no requirement for such documents has been identified. It may however be the case that specifications for conformity checker tools could be identified in the future such as conformity 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		19	5	0	0	Business Driven Guidance for Trust Application Service Providers
SR		19	5	3	0	Study on standardisation requirements for e-Delivery services applying e-Signatures
				Policy & Security Requirements		
EN		19	5	1	1	Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers
EN		19	5	2	1	Policy & Security Requirements for Data Preservation Service Providers (DPSPs)
				Technical Specifications		
EN		19	5	1	2	Registered Electronic Mail (REM) Services
EN		19	5	2	2	Data Preservation Services through signing
				Conformity Assessment		
EN		19	5	1	3	Conformity Assessment for REM Service Providers
EN		19	5	2	3	Conformity Assessment of Data Preservation Service Providers
				Testing Compliance & Interoperability		
TS		19	5	0	4	General requirements for Testing Compliance & Interoperability of TASPs
TS		19	5	1	4	Testing Compliance & Interoperability of REM Service Providers

Guidance

TR 19 500 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.

SR 19 530 Study on standardisation requirements for e-Delivery services applying e-Signatures

This document will define Electronic Delivery (e-delivery) services and investigate applicable requirements from those existing in the market (ETSI, CEN, private standards and pilots' outcome) proposing rationalised and well organized requirements for Electronic Delivery Applying Electronic Signatures and its possible relation to Registered E-Mail.

Policy & Security Requirements

EN 19 511 Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers

This document specifies policy and security requirements for REM service providers required to be recognized as a provider of this type of services. It might define different conformity 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 REM systems. It references EN 19 501 for generic requirements.

NOTE: Whether a "Security (Protection) Profile for Trustworthy systems used by REM Service Providers" should be merged within those specific policy & security requirements is yet to be further analysed.

This multi-part document includes:

- Overview. This part provides an overview of the other parts of this document. It also describes the relationship of the policy requirements defined in this area and the use of secure devices and trustworthy systems defined in the "Signature Creation and Other Related Device" area.
- Policy requirements for REM Service Providers.

Informative annexes will provide check lists for conformity assessment.

EN 19 521 Policy & Security Requirements for Data Preservation Service Providers (DPSPs)

This document specifies policy and security requirements for DPSPs. It references EN 19 501 for generic requirements.

It may address specific Information Security Management Systems or Data Preservation Systems (DPS), by specifying specific security requirements for Data Preservation Service Providers to abide by, when implementing and managing a DPS, in order to provide Data Preservation Services that are trustable and reliable from the Information Security viewpoint. This document does not address any archival specific issues, like definition of data metadata structure and methods to build them, links between data to implement virtual folders, etc.

NOTE: Whether a "Security (Protection) Profile for Trustworthy systems used by Data Preservation Service Providers" should be merged within those specific policy & security requirements is yet to be further analysed.

This multi-part document includes:

- Overview. This part provides an overview of the other parts of this document. It also describes the relationship of the policy requirements defined in this area and the use of secure devices and trustworthy systems defined in the "Signature Creation and Other Related Devices" area.
- Policy requirements for Data Preservation Service Providers.

Informative annexes will provide check lists for conformity assessment.

Technical Specifications

EN 19 512 Registered Electronic Mail Services

This document provides technical specifications for the provision of Registered Electronic Mail. This is a multi-part document whose structure is detailed below:

- **Framework, Architecture and Evidence:** This is a document structured in three sub-parts, as detailed below:
  - **Registered Electronic Mail 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 1: Its internal structure will very much depend on the different relevant systems specified and built across Europe, as during the last years a number of specifications and non interoperable systems based on them, have been developed.

NOTE 2: Requirements for support of Registered Electronic Delivery requires further investigation.

SR 19 522 Data Preservation Services through signing

This document specifies technical requirements for services providing document signing in support of data 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. An initial study will identify standardisation requirements and how this relates to general standardisation for archiving and data preservation.

Conformity Assessment

EN 19 513 Conformity Assessment of Registered Electronic Mail Service Providers

This document specifies requirements and provides guidance for the supervision and assessment of a Registered Electronic Mail Service Provider based on general requirements and guidance for conformity assessment specified in EN 19 403.

EN 19 523 Conformity Assessment of Data Preservation Service Providers

This document specifies requirements and provides guidance for the supervision and assessment of a DPSP based on general requirements and guidance for conformity assessment specified in EN 19 403.

Testing Compliance & Interoperability

TS 19 504 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 19 514 Testing Compliance & Interoperability of Registered Electronic Mail 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 is 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 is for those providers that implement the service provision using different combinations of format and transport protocols. This document defines test-suites for the interoperability profiles for REM.
- **Testing compliance:** This document specifies the tests to be performed for checking conformity against EN 19 512. This provides the basis for a tool that automatically checks 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	19	6	0	0	Business Driven Guidance for Trust Service Status Lists Providers
					Policy & Security Requirements
EN	19	6	0	1	General Policy & Security Requirements for Trust Service Status Lists Providers (TSSLPs)
EN	19	6	1	1	Policy & Security Requirements for Trusted Lists Providers
					Technical Specifications
EN	19	6	0	2	Trust Service Status Lists Format
EN	19	6	1	2	Trusted Lists Format
					Conformity Assessment
EN	19	6	0	3	General requirements and guidance for Conformity Assessment of TSSLPs
EN	19	6	1	3	Conformity Assessment of Trusted List Providers
					Testing Compliance & Interoperability
TS	19	6	0	4	General requirements for Testing Compliance & Interoperability of TSSLPs
TS	19	6	1	4	Testing Compliance & Interoperability of Trusted Lists

Guidance

TR 19 600 Business Driven Guidance for Trust Service Status Lists Providers

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

Policy & Security Requirements

EN 19 601 General Policy & Security Requirements for Trust Service Status Lists Providers

This document specifies general policy and security 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 19 611 Policy & Security Requirements for Trusted List Providers

This document specifies specific policy requirements for issuers of Trusted List, a profile of Trust Service Status List, as they are defined in CD 2009/767/EC [i.19] as amended by CD 2010/425/EU [i.20]. This would build on the requirements in EN 19 601.

Technical Specifications

EN 19 602 Trust Service Status Lists Format

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 Lists 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 Lists**
  This part specifies the ASN.1 structures to be used when implementing an ASN.1-version of TSLs.

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

EN 19 612 Trusted List Format

This document contains all the specifications related to Trusted Lists, a profile of Trust Service Status List, for their use in the context of Directive 1999/93/EC [i.1] and of the Services Directive 2006/123/EC [i.14], 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 use of EN 19 602 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 European 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 Europe-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 19 602 would be required.

Conformity Assessment

EN 19 603 General requirements and guidance for Conformity Assessment of TSSLPs

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

EN 19 613 Conformity Assessment of Trusted List Providers

This document specifies the specific conformity rules for assessing conformity against EN 19 612 specifications related to both the generation and conformity validation of Trusted Lists, a profile of Trust Service Status Lists.

Testing Compliance & Interoperability

TS 19 604 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 19 602. This is a multi-part 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 19 602.

- **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 19 602.

TS 19 614 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 19 612.
- **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 & Work Plan

6.1 Methodology

The analysis and resulting work plan are placed in a set of tables bringing the gap analysis and work plan together on a per document basis in tables showing:

a) The analysis of the required scope of each document identified in the rationalised structure against the currently available specification (including those shortly to become available through quick fixes) identifying those whose scope most closely matches that of the required scope.

b) The work plan required to produce the required document from the currently available specifications.

The analysis identifies the existing documents from the inventory whose scope is near that of the required document in the rationalised framework and indicates the degree to which the requirements are met as follows:

1) Scope fully met: A document already exists, either from inventory or quick fix, at the level of standardisation needed and with the required scope.

2) Scope nearly met: A document already exists, either from inventory or quick fix, but requires some minor enhancements to fulfil the required scope and / or completion of progression to the required level of standardisation (e.g. finalising EN).

3) Requirement partially met: A document already exists but some enhancements are needed to meet the required scope and/or the standardisation level is not sufficient.

4) Inputs exist: Documents exist in the inventory which could be used as the basis of the required standard but significant work is required to bring the document to the required level of standardisation addressing the identified scope.

5) Little basis: There is little basis for this document required.

The work plan identifies the tasks to be carried out to produce a document of the required scope and an indication or the expected time-scale.

6.2 Analysis and Work Plan by Area

NOTE: In the following work plan timescale T0 is the start of Phase 2 activities (after specialist task forces/project teams have been set up by CEN/ETSI) currently estimated to be September 2012. Prior to T0 there is expected to be a 3 month period for project set up. Thus it is assumed that the European Commission gives notification to start phase 2 of Mandate 460 in June 2012.

6.2.1 Generic

Summary

Table 7: Work Plan summary for Guidance on Rationalised Structure

					Rationalised structure for Electronic Signature Standardisation	Degree scope met	Starting Points
					Sub-areas		
					Guidance		
TR	19	0	0	0	Rationalised structure for Electronic Signature Standardisation	Partially met	SR-ESI-000099
SR	19	0	1	0	Extended Rationalised structure including IAS	Little basis	SR-ESI-000099

Details

Deliverable id	Type	Title and Contents
		GUIDANCE
19000	TR	**Title: Rationalised structure for Electronic Signature Standardisation**
		Description: This document is to provide the framework for the 19 000 series of documents on Electronic Signature standardisation.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: • Starting points: The present document section 5 • Other documents: Assurance levels identified by IAS study, ISO DIS 29115, CROBIES WP5.2
		WORK PLAN **Task to be carried out**: • Production of a new document TR based the present document • **SR 19010**: Study on the extension of the rationalised framework to support emerging technologies and support for Identification Authentication and Signatures **Timescale** (planning): • Start: T0 • Complete: T0 + 12

6.2.2 Signature Creation and Validation

Summary

Table 8: Work Plan summary for Standards for Signature Creation and Validation

		Signature Creation and Validation						
		Sub-areas						
					Guidance			
TR	19	1	0	0	Business Driven Guidance for Signature Creation and Validation	Inputs exist	TR 102045, CROBIES WP5.1, SR-ESI 000099
					Policy & Security Requirements			
EN	19	1	0	1	Policy & Security Requirements for Signature Creation and Validation	Inputs exist	none
EN	19	1	1	1	Protection Profiles for Signature Creation and Validation Application	Nearly met	prEN 14170-1/5
					Technical Specifications			
EN	19	1	0	2	Procedures for Signature Creation and Validation	Partially met	TS-ESI-000074
EN	19	1	2	2	CAdES - CMS Advanced Electronic Signatures	Nearly met	TS 101733, TS 103173, TS102734, ISO 14533-1
EN	19	1	3	2	XAdES - XML Advanced Electronic Signatures	Partially met	TS 101903, TS 103171, TS102904,
EN	19	1	4	2	PAdES - PDF Advanced Electronic Signatures	Nearly met	TS 102778, TS 103172, TS102904, ISO 32000
EN	19	1	5	2	Advanced Electronic Signatures in Mobile environments	Inputs exist	TS 102207, TS 102204, TR 102 203, TR 102207
EN	19	1	6	2	ASiC - Associated Signature Containers	Partially met	TS 102918, TS 103174
EN	19	1	7	2	Signature Policies	Inputs exist	CROBIES WP5.1, TR 102045, TR 102038, TR 102272
					Conformity Assessment			
EN	19	1	0	3	Conformity Assessment for Signature Creation & Validation Applications (& Procedures)	Little basis	CWA 14172-4
					Testing Compliance & Interoperability			
TS	19	1	0	4	General requirements on Testing Compliance & Interoperability of SC&V	Little basis	none
TS	19	1	2	4	CAdES Testing Compliance & Interoperability	Partially met	*See EN 66122 + outcome of STF428 & STF426 1 former interoperability events*
TS	19	1	3	4	XAdES Testing Compliance & Interoperability	Partially met	*See EN 66132 + outcome of STF428 & STF426 1 former interoperability events*
TS	19	1	4	4	PAdES Testing Compliance & Interoperability	Partially met	*See EN 66142 + outcome of STF428 & STF426 1 former interoperability events*
TS	19	1	5	4	Testing Compliance & Interoperability of AdES in Mobile environments	Little basis	*See EN 66152 + outcome of STF428 & STF426 1 former interoperability events*
TS	19	1	6	4	ASiC Testing Compliance & Interoperability	Partially met	*See EN 66162 + outcome of STF428 & STF426 1 former interoperability events*
TS	19	1	7	4	Testing Compliance & Interoperability of Signature Policies	Little basis	*See EN 66172 + outcome of STF428 & STF426 1 former interoperability events*

Details

Deliverable id	Type	Title and Contents
		GUIDANCE
19100	TR	**Title: Business Driven Guidance for Signature Creation and Validation**
		Description: This document provides business guidance for use of electronic signature standards 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.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: • Starting points: TR 102 045, CROBIES WP5.1, DSR-ESI-00099 (annex B) • Other documents: ISO 15944-5, CWA 14708, ITU-T Draft X.1254/ISO DIS 29115, 19 000 • Reasons why selecting starting points: Existing and previous related works • Degree to which scope is met considering starting points: o Input exists (see annex B)
		WORK PLAN **Task to be carried out**: • Production of a new document TR based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning): • Start: T0 • Complete: T0 + 12
		POLICY AND SECURITY REQUIREMENTS
19 101	EN	**Title: Policy and Security Requirements for Electronic Signature Creation and Validation**
		Description: 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 19172).
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: • Starting points: none • Other documents: Belgium Industry Best Practice for Applications using the electronic Identity Card, TR 102 045, TR 102 038, TR 102 041, TR 102 272, ISO 15408, ISO 15443, CWA 14365-1, CWA 14171 • Reasons why selecting starting points: existing related works • Degree to which scope is met considering starting points (choice) o Input exists
		WORK PLAN **Task to be carried out**: • Production of a new EN document based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning): • Start: T0 • Complete: T0+24
19 111	EN	**Title: Protection Profile for Electronic Signature Creation and Validation**
		Description: This multi-part document specifies the security requirements for signature creation and validation applications. This includes security requirements on mandatory core functions of signature creation and validation applications as well as security requirements for possible extensions to the core functions.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: • Starting points: CEN prEN 14170-1 to 14170-5 • Other documents: ISO 15446, CWA 14365-2, CWA 14170. • Reasons why selecting starting points: matches scope • Current Draft EN 14 170 contains Protection Profiles that define the security requirements for Signature Creation Applications (SCA) and Signature Validation applications (SVA). – Part 1 is an introduction to the EN: This part is an introduction to the European Norm that contains Protection Profiles that define the security requirements for Signature Creation and Signature Validation applications. It defines terms used in all parts. §2 describes the SCA, its functions, its environment. §3 describes the SVA, its functions, its environment. – Part 2 is the core PP for an SCA: This PP aims at defining security requirements for SCA conformity from the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to software, running on an operating system and hardware, the Signature Creation Platform. The TOE, using services provided by the Signature Creation Platform and by an SSCD allows the signatory to generate an electronic signature. – Part 3 proposes extensions to Part 2. – Part 4 is the core PP for an SVA: This PP aims at defining security requirements for SVA conformity from the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to software, running on an operating system and hardware, the Signature Validation Platform. The TOE, using services provided by the Signature Validation Platform and by the environment allows the verifier to check an electronic signature. – Part 5 proposes extensions to Part 4. • Degree to which scope is met considering starting points o Scope nearly met
		WORK PLAN **Task to be carried out:** • Production of an EN from an existing document with minor updates **Timescale** (planning): • Start: In progress • Complete: 2013
TECHNICAL SPECIFICATIONS		
19 102	EN	**Title: Procedures for Signature Creation and Validation**
		Description: This document specifies procedures for creation and validation of an Advanced Electronic Signature within a given policy context.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: The ETSI TS that will be completed under **WI DTS/ESI-000074** • Other documents: RFC 5914, RFC 5280, RFC 4158, RFC 3161, RFC 2560, RFC 5816 RFC 5019, RFC 5652, XML TimeStamping Profile of the OASIS DSS, RFC 3281, RFC 3739, ISO18014, ETSI TS 101 861, ,ETSI TS 101 862, ETSI TR 101 272, ETSI TS 102 280, TR 102 047, CEN CWA 14172-4, CEN CWA 14171. OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Validation Reports. • Reasons why selecting starting points: This document will specify the core algorithm for verifying AdES signatures. Signature creation part should be added. • Degree to which scope is met considering starting points: **Scope partially met**. The EN to be produced will have to additionally take into account the role of European Trusted Lists in the validation process. Additionally, this EN will have to specify rules for verifying applications when they decide to neglect certain signature components in the validation process (transparency rules). No material existing regarding procedures for signature creation.

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out**: • Production of a new EN document based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning): • Start: T0 • Complete: T0+18
19 122	EN	**Title: CMS Advanced Electronic Signature Formats (CAdES)**
		Description: 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.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI TS 101 733 (CAdES mother specification), ETSI TS 103 173 CAdES Baseline Profile), ETSI TS 102 734, ISO 14533-1: Long term signature profiles for CAdES. • Other documents: RFC 5126, RFC 5652, ITU-T X.680, ITU-T X.690, RFC 5280, RFC 2634, RFC 3161, RFC 2560, RFC 5816 RFC 5019, RFC 5652, XML TimeStamping Profile of the OASIS DSS, RFC 3281, RFC 3739, ETSI TS 101 861,ETSI TS 101 862, ETSI TR 101 272, ETSI TS 102 280, TR 102 047, CEN CWA 14172-4, CEN CWA 14171. • Reasons why selecting starting points: The 4 identified documents are the CAdES mother specifications and three documents containing different profiles. The final EN is to be a multi-part document including CAdES mother specification and a set of profiles already identified as relevant. • Degree to which scope is met considering starting points: At present each part of the final European Norm is in a different status. Details for each one are listed below: o **CAdES mother specification**: **Scope nearly met**. o **CAdES Baseline Profile**: **Scope fully met when WI RTS/ESI-000105**. Only process comments received from stakeholders after using conformity testing tools and participating in interoperability test events. o **CAdES e-Invoicing Profile**: **Partially met**. It has been long time since the ETSI TS 102 734 was firstly published. This spec took into account situation regarding implementations and requirements at that point in time, which will have very likely changed very much since then. This needs to be built upon the baseline profile.
		WORK PLAN **Task to be carried out:** Details are listed below regarding the different parts of the final EN: • **CAdES mother specification:** Production of an EN from an existing document with minor updates. • **CAdES Baseline Profile:** Progression of an existing (proposed draft) TS to a full EN within Rationalised Framework classification. • **CAdES e-Invoicing Profile:** Production of a new EN document without existing documents to be based on (incl. stakeholder consultation) **Timescale** (planning): • Start: T0 • Complete: T0+24
19 132	EN	**Title: XML Advanced Electronic Signature Formats (XAdES)**
		Description: 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.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI TS 101 903 (XAdES mother specification), ETSI TS 103 171 (XAdES Baseline Profile), ETSI TS 102 904 (several initial XAdES profiles, including e-Invoicing, e-Government), ISO 14533-2: Long term signature profiles for XAdES, W3C XML Signature Syntax and Processing version 1.0, W3C XML Signature Syntax and Processing version 1.1 (a Candidate Recommendation when this report is written), W3C XML Signature Syntax and Processing 2.0 (Working Draft status when this report is written). • Other documents: W3C Canonical XML V 1.0, W3C Exclusive XML Canonicalization v 1.0, W3C Canonical XML: v 1.1, XML-Signature Xpath Filter 2.0, XML Path Language (XPath) v.10, XSL Transformations Version 1.0, W3C XML Signature Properties, RFC 5280, RFC 3161, RFC 2560, RFC 5816 RFC 5019, XML TimeStamping Profile of the OASIS DSS, RFC 3281, RFC 3739, ETSI TS 101 861,ETSI TS 101 862, ETSI TR 101 038, ETSI TS 102 280, TR 102 047, CEN CWA 14172-4, CEN CWA 14171, ITU-T X.680, ITU-T X.690. Web Services Security: SOAP Message Security 1.0, W3C XML Signature Syntax and Processing version 1.0 • Reasons why selecting starting points: The 4 identified ETSI documents are the XAdES mother spec and three documents containing different profiles. The final EN is to be a multi-part document including XAdES mother specification and a set of profiles already identified as relevant. In addition to that, the two XML Sig W3C specifications, when arrived to W3C Recommendation status, will be format on which future XAdES signatures will be built. • Degree to which scope is met considering starting points: At present each part of the final European Norm is in a different status. Details for each one are listed below: o **XAdES mother specification**: **partially met.** Changes in W3C XML Sig makes it worth to discuss with more details the different degrees of scope fulfilment as it is foreseen that the final XAdES mother specification specifies how to build XAdES signatures on the different XML Sig versions, not only on one: ▪ **XAdES built on W3C XML Sig version 1.1: scope partially me**t. Alignment of XAdES specification to ensure correct usage of this XML Sig version. ▪ **XAdES built on W3C XML Sig version 2.0: Little basis**. This version of XML Sig incorporates an alternative mechanism for referencing signed data objects while preserving backwards compatibility. Careful study on impact on XAdES is required. ▪ **XAdES built on W3C XML Sig version 1.0: scope nearly met**. Regarding the evolution of traditional XAdES, a number of improvements are required, among which: o **XAdES Baseline Profile**: **Scope fully met when WI RTS/ESI-000103 is complete**. Only process comments received from stakeholders after using conformity testing tools and participating in interoperability test events. o **XAdES e-Invoicing Profile**: **partially met**. It has been long time since the ETSI TS 102 904 was firstly published. This spec took into account situation regarding implementations and requirements at that point in time, which will have very likely changed very much since then. This needs to be built upon the baseline profile.

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out:** Details are listed below regarding the different parts of the final EN: • **XAdES mother specification aligned with XML Sig v1.0**. Production of an EN from an existing document with minor updates. • **XAdES mother specification aligned with XML Sig v1.1**. Significant revision to an existing document (before progression to EN). • **XAdES mother specification aligned with XML Sig v2.0**. Significant revision to an existing document (before progression to EN). • **XAdES Baseline Profile**. Progression of an existing (proposed draft) EN to a full EN within Rationalised Framework classification. • **XAdES e-Invoicing Profile**. Production of a new document (e.g. EN, TS) without existing documents to be based on (incl. stakeholder consultation) **Timescale** (planning): • Start: T0 • Complete: .T0+24
19 142	EN	**Title: PDF Advanced Electronic Signature Formats (PAdES)**
		Description: 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.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI TS 102 778 (PAdES mother specification in its parts 1 to 6), ETSI TS 103 172 (PAdES Baseline Profile), ISO 32000: PDF specification. • Other documents: RFC 5126, RFC 5652, ITU-T X.680, ITU-T X.690. RFC 5280, RFC 2634, RFC 3161, RFC 2560, RFC 5816 RFC 5019, RFC 5652, XML TimeStamping Profile of the OASIS DSS, RFC 3281, RFC 3739, ETSI TS 101 861,ETSI TS 101 862, ETSI TR 101 272, ETSI TR 101 038, ETSI TS 102 280, TR 102 047, CEN CWA 14172-4, CEN CWA 14171, W3C Canonical XML V 1.0, W3C Exclusive XML Canonicalization v 1.0, W3C Canonical XM: v 1.1, XML-Signature Xpath Filter 2.0, XML Path Language (XPath) v.10, XSL Transformations (Version 1.0, W3C XML Signature Properties. • Reasons why selecting starting points: The 2 ETSI identified documents are the PAdES mother spec and the PAdES Baseline Profile. The final EN is to be a multi-part document including PAdES mother specification and a set of profiles already identified as relevant. • Degree to which scope is met considering starting points: At present each part of the final European Norm is in a different status. Details for each one are listed below: o **PAdES mother specification: Scope nearly met**. Only required process comments received from implementers and participants in interoperability test events. o **PAdES Baseline Profile: Scope fully met when WI RTS/ESI-000104 is complete**. Only process comments received from stakeholders after using conformity testing tools and participating in interoperability test events. o **PAdES e-Invoicing Profile: Little basis**. There was not even a previous profile for e-Invoicing as happens with XAdES and CAdES.

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out:** Details are listed below regarding the different parts of the final EN: • **PAdES mother** specification**:** Production of an EN from an existing document with minor updates • **PAdES Baseline Profile:** Progression of an existing (proposed draft) EN to a full EN within Rationalised Framework classification • **PAdES e-Invoicing Profile:** Production of a new document (e.g. EN, TS) without existing documents to be based on (incl. stakeholder consultation) **Timescale** (planning)**:** • Start T0 • Complete: T0+24
19 152	EN	**Title: Advanced Electronic Signatures in Mobile environments**
		Description: This document will provide details on the framework (including architecture and relevant scenarios) required for the management of Advanced Electronic Signatures in Mobile environments.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI TS 102 207, ETSI TS 102 204, ETSI TR 102 203, ETSI TS 102 206 • Other inputs: MOA-SS/SP, MOA-Amtssignature-MOA-AS Specification • Reasons why selecting starting points: ETSI specifications formalizing the concept • Degree to which scope is met considering starting points: input exists
		WORK PLAN **Task to be carried out:** Production of the EN after taking into consideration not only ETSI Technical Specifications and Technical Reports, but also other already existing specifications, especially if they have been implemented. **Timescale** (planning)**:** • Start: T0 • Complete:T0+24
19 162	EN	**Title: Associated Signature Containers (ASiC)**
		Description: This document contains all the specifications related to the so-called Associated Signature Container. This is a multi-part document that includes the base specification and associated profiles.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI TS 102 918 (ASiC mother), ETSI TS 103 174 (ASiC Baseline Profile). • Other documents: IDPF "OEBPS Container Format", PKWARE: ".ZIP Application Note), OASIS: "Open Document Format for Office Applications (OpenDocument) Version 1.2. Part 3: Packages, RFC 5126, RFC 5652, ITU-T X.680, ITU-T X.690. RFC 5280, RFC 2634, RFC 3161, RFC 2560, RFC 5816 RFC 5019, RFC 5652, XML TimeStamping Profile of the OASIS DSS, RFC 3281, RFC 3739, ETSI TS 101 861,ETSI TS 101 862, ETSI TR 101 272, ETSI TR 101 038, ETSI TS 102 280, TR 102 047, CEN CWA 14172-4, CEN CWA 14171, W3C Canonical XML V 1.0, W3C Exclusive XML Canonicalization v 1.0, W3C Canonical XM: v 1.1, XML-Signature Xpath Filter 2.0, XML Path Language (XPath) v.10, XSL Transformations Version 1.0, W3C XML Signature Properties. • Reasons why selecting starting points: The 2 identified documents are the ASiC mother spec and the ASiC Baseline Profile. The final EN is to be a multi-part document including ASiC mother specification and a set of profiles already identified as relevant. • Degree to which scope is met considering starting points (choice). At present each part of the final European Norm is in a different status. Details for each one are listed below: o **ASiC mother specification**: **Scope partially met:** The current specification does not deal with signatures archival. A work item is on-going for fulfilling this requirement. In addition to that comments received by implementers after using conformity testing tools and participating in interoperability test events will need to be processed.. o **ASiC Baseline Profile**: **Scope fully met when WI RTS/ESI-000106 is complete:** Only process comments received from stakeholders after using conformity testing tools and participating in interoperability test events. o **ASiC e-Invoicing Profile**: **Input exists:** It is expected though that the work on e-Invoicing profiles for XAdES and CAdES will also constitute input for developing this profile.
		WORK PLAN **Task to be carried out:** Details are listed below regarding the different parts of the final EN: • **ASiC mother** specification**:** Production of an EN from an existing document with minor updates. • **ASiC Baseline Profile:** Progression of an existing (proposed draft) EN to a full EN within Rationalised Framework classification. • **ASiC e-Invoicing Profile:** Production of a new document (e.g. EN, TS) without existing documents to be based on (incl. stakeholder consultation) **Timescale** (planning) **:** • Start: T0 • Complete: T0+24
19 172	EN	**Title: Signature Policies**
		Description: This document fully addresses signature policies to be used in the management of electronic signatures within extended business models.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: CROBIES WP5.1, ETSI TR 102 045. Signature Policy for extended business model, ETSI TR 102 038: XML Format for signature policies, ETSI TR 102 272: ASN.1 Format for signature policies. • Other documents: RFC 3647. • Reasons why selecting starting points: The above two last TRs specify XML and ASN.1 formats for signature policies. They should constitute the starting point for specifying formats that may be processed by machines, even if latest advancements in XML languages lead to substantially different final languages. The two first documents should constitute the starting point for actually scoping the concept of Signature Policy and for identifying semantic requirements matched to business needs. • Degree to which scope is met considering starting points: At present each part of the final European Norm is in a different status. Details for each one are listed below: o **Signature policies: Input exists:** CROBIES WP5.1 should be taken into account as a basis for such a work as it already constitutes a significant update from ETSI TR 102 045 (full reworking of the human readable format should be done). o **XML format for Signature Policies**: **Input exists:** An on-going work **(WI RTS/ESI-000114)** is being made for evolving TR 102 038 to TS. This should be the starting point, as well as the outcome of the previous part, which could lead to a new XML language for Signature policies. o **ASN.1 format for Signature Policies**: **Input exists:** An on-going work **(WI RTS/ESI-000102)** is being made for evolving TR 102 272 to TS. This should be the starting point, as well as the outcome of the previous part, which could lead to a new ASN.1 language for Signature policies.
		WORK PLAN **Task to be carried out:** Details are listed below regarding the different parts of the final EN: • **Human readable**. Production of a new EN document based on a number of existing documents (incl. stakeholder consultation) • **XML format for Signature Policies**. Significant revision to an existing document (before progression to EN). • **ASN.1 format for Signature Policies**. Significant revision to an existing document (before progression to EN). **Timescale** (planning)**:** • Start:T0 • Complete: T0+24
CONFORMITY ASSESSMENT		
19 103	EN	**Title: Conformity Assessment for Signature Creation and Validation Applications (and Procedures)**
		Description: This document addresses the entire process for performing complete assessment of SCA/SVA against Policy Requirements and/or Protection Profiles, AdES technical specifications, formats and protocols; and for complete assessment of a specific machine processable signature policy against the business process policy requirements.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: • Starting points: CWA 14172-4 • Other documents: none • Reasons why selecting starting points: n.a. • Degree to which scope is met considering starting points: o Little basis

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out**: • Production of a new document (e.g. EN, TS) without existing documents to be based on (incl. stakeholder consultation) **Timescale** (planning): • Start: T0 • Complete: T0 + 24 months
		TESTING COMPLIANCE AND INTEROPERABILITY
19 104	TS	**Title: General requirements on Testing Compliance and Interoperability of Signature Creation and Validation**
		Description: This set of documents specifies general requirements for testing compliance and interoperability of signature creation and validation applications**.**
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: None. • Other documents: o ETSI TS under production ETSI TC ESI: "Conformity Testing for XAdES Baseline Profile" **(WI DTS/ESI-000095)**. o ETSI TS under production: "Test Suite for PDF Advanced Signatures (PAdES) interoperability test events" " **(WI DTS/ESI-000096)**. o ETSI TS under production: "Test Suite for Associated Signature Containers (ASiC) interoperability test events". (**WI DTS/ESI-000097)**. o Test suites for XAdES as developed for XAdES interoperability events. • Degree to which scope is met considering starting points: **Little Basis.**
		WORK PLAN **Task to be carried out:** • Production of a new TS document without existing documents to be based on (incl. stakeholder consultation). **Timescale** (planning)**:** • Start: T0+6 • Complete: T0+24
19 124	TS	**Title: CAdES Testing Compliance & Interoperability**
		Description: This document will firstly 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.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: o Same as starting points for CAdES EN 19 122. o RFC 5652: CMS • Other documents: o ETSI TS under production by ETSI TC ESI: "Conformity Testing for XAdES Baseline Profile" **(WI DTS/ESI-000095)**. o ETSI TS under production: "Test Suite for PDF Advanced Signatures (PAdES) interoperability test events" " **(WI DTS/ESI-000096)**. o ETSI TS under production: "Test Suite for Associated Signature Containers (ASiC) interoperability test events". (**WI DTS/ESI-000097)**. o Test suites for XAdES as developed for XAdES interoperability events. • Reasons why selecting starting points: The whole package of CAdES specifications including mother specification and its profiles, are required for defining the complete set of conformity test suite as well as for defining adequate and as much complete as possible test suites for interoperability tests. • Degree to which scope is met considering starting points: The current situation is different regarding the actual technical specification and whether conformity or interoperability testing is addressed. Details are provided below: o **Test suites for testing interoperability for CAdES signatures**: **Scope nearly met**. Two interoperability events have already been conducted for CAdES. Test suites already defined. New test suites should be defined for the profiles. o **Specifications for testing compliance of CAdES Signatures: Little basis**. This is a document that will have to be started from the scratch. Experience will exist in developing such specification once the ETSI TC ESI will have finished similar TS for testing conformity for XAdES baseline profile **(WI DTS/ESI-000095).**
		WORK PLAN **Task to be carried out:** Details are listed below regarding the different parts of the final TS: • **Test suites for testing interoperability for CAdES signatures**. Production of TS from an existing document with minor updates. • **Specifications for testing compliance of CAdES Signatures**. Production of a new TS document without existing documents to be based on (incl. stakeholder consultation). **Timescale** (planning)**:** • Start: T0+6 • Complete: T0+24
19 134	TS	**Title: XAdES Testing Compliance & Interoperability**
		Description: This document will firstly 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.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: o Same as starting points for XAdES EN 19 132. o W3C XML Sig versions 1.0, 1.1 and 2.0 o ETSI TS under production by ETSI TC ESI: "Conformity Testing for XAdES Baseline Profile" **(WI DTS/ESI-000095)**. o Test suites for XAdES as developed for XAdES interoperability events. • Other documents: o ETSI TS under production: "Test Suite for PDF Advanced Signatures (PAdES) interoperability test events" " **(WI DTS/ESI-000096)**. o ETSI TS under production: "Test Suite for Associated Signature Containers (ASiC) interoperability test events". (**WI DTS/ESI-000096)**. • Reasons why selecting starting points: The whole package of XAdES specifications including mother specification and its profiles, as well as the different versions of XML Sig, are required for defining the complete set of conformity test suite as well as for defining adequate and as much complete as possible test suites for interoperability tests. The test suites defined for XAdES interoperability events will be the core content for formalizing this part of the TS. Finally the TS to be produced by the ETSI TC ESI will be the starting point at the core of the conformity testing part. • Degree to which scope is met considering starting points: The current situation is different regarding the actual technical specification and whether conformity or interoperability testing is addressed. Details are provided below: o **Test suites for testing interoperability for XAdES signatures**: **Scope partially met**. Several interoperability events have already been conducted for XAdES. Test suites already defined, including evolution and arbitration of XAdES signatures. Experience for formalizing tests suites in Technical Specifications will be provided by the TSs defining test suites for PAdES and ASiC as produced by ETSI TC ESI. Nevertheless, new versions of XML Sig will need to be taken into account. o **Specifications for testing compliance of XAdES Signatures: Scope partially met**. The TS for testing conformity for XAdES baseline profile **(WI DTS/ESI-000095)** will be at the core of this set of test suites, as a good part of them will be common to the XAdES mother specification and the XAdES baseline and e-Invoicing profiles. As before, though, new versions of XML Sig will have to be taken into account.
		WORK PLAN **Task to be carried out**: Details are listed below regarding the different parts of the final TS: • **Test suites for testing interoperability for XAdES signatures**. Production of a new TS document based on a number of existing documents (incl. stakeholder consultation). • **Specifications for testing compliance of XAdES Signatures**. Production of a new TS document based on a number of existing documents (incl. stakeholder consultation). **Timescale** (planning): • Start: T0+6 • Complete: T0+24
19 144	TS	**Title: PAdES Testing Compliance & Interoperability**
		Description: This document will firstly 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.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: o Same as starting points for PAdES EN 19 142. o ISO 32000 o ETSI TS under production: "Test Suite for PDF Advanced Signatures (PAdES) interoperability test events" **(WI DTS/ESI-000096)**. • Other documents: o ETSI TS under production by ETSI TC ESI: "Conformity Testing for XAdES Baseline Profile" **(WI DTS/ESI-000095)**. • Reasons why selecting starting points: The whole package of PAdES specifications including mother specification and its profiles, as well as ISO 32000, are required for defining the complete set of conformity test suite as well as for defining adequate and as much complete as possible test suites for interoperability tests. The test suites defined for PAdES interoperability events by ETSI will be the starting point at the core of the interoperability testing part. • Degree to which scope is met considering starting points: The current situation is different regarding the actual technical specification and whether conformity or interoperability testing is addressed. Details are provided below: o **Test suites for testing interoperability for PAdES signatures**: **Scope fully met when ETSI will complete the ETSI TS "Test Suite for PDF Advanced Signatures (PAdES) interoperability test events**". Only required process comments received from implementers and participants in interoperability test events.. o **Specifications for testing compliance of PAdES Signatures: Little basis**. This is a document that will have to be started from the scratch. Experience will exist in developing such specification once the ETSI will have finished similar TS for testing conformity for XAdES baseline profile **(WI DTS/ESI-000095).**
		WORK PLAN **Task to be carried out**: Details are listed below regarding the different parts of the final TS: • **Test suites for testing interoperability for PAdES signatures**. Production of TS from an existing document with minor updates. • **Specifications for testing compliance of PAdES Signatures**. Production of a new TS document without existing documents to be based on (incl. stakeholder consultation). **Timescale** (planning): • Start: T0+6 • Complete: T0+24

Deliverable id	Type	Title and Contents
19154	TS	**Title: Testing Compliance & Interoperability of AdES in Mobile environments**
		Description: This document will firstly define test suites as completely as possible for supporting the organization of interoperability testing events where different AdES related applications in Mobile environments may check their actual interoperability. Additionally, it will include the specifications required for building up software tools for actually testing technical compliance of AdES in Mobile environment against the relevant related technical specifications.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: Same as starting points for EN 19 152. • Other documents: none • Reasons why selecting starting points: existing documents • Degree to which scope is met considering starting points: **Little basis**
		WORK PLAN **Task to be carried out:** exploratory study **Timescale** (planning): • Start: T0+6 • Complete: T0+24
19 164	TS	**Title: ASiC Testing Compliance & Interoperability**
		Description: This document will first define test suites as much complete as possible for supporting the organization of interoperability testing events where different ASiC 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 implementations against the relevant ASiC related technical specifications.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: o Same as starting points for ASiC EN 19 162. o ETSI TS under production: "Test Suite for Associated Signature Containers (ASiC) interoperability test events" **(WI DTS/ESI-000097)**. • Other documents: o ETSI TS under production ETSI TC ESI: "Conformity Testing for XAdES Baseline Profile" **(WI DTS/ESI-000095)**. • Reasons why selecting starting points: The whole package of ASiC specifications including mother specification and its profiles, are required for defining the complete set of conformity test suite as well as for defining adequate and as much complete as possible test suites for interoperability tests. The test suites defined for ASiC interoperability events by ETSI will be the starting point at the core of the interoperability testing part. • Degree to which scope is met considering starting points: The current situation is different regarding the actual technical specification and whether conformity or interoperability testing is addressed. Details are provided below: o **Test suites for testing interoperability for ASiC**: **Scope fully met** when ETSI TC ESI will complete the ETSI TS "Test Suite for Associated Signature Containers (ASiC) interoperability test events". Only required process comments received from implementers and participants in interoperability test events. o **Specifications for testing compliance of ASiC: Little basis**. This is a document that will have to be started from the scratch. Experience will exist in developing such specification once ETSI will have finished similar TS for testing conformity for XAdES baseline profile **(WI DTS/ESI-000095).**

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out**: Details are listed below regarding the different parts of the final TS: • **Test suites for testing interoperability for ASiC**. Production of TS from an existing document with minor updates. • **Specifications for testing compliance of ASiC**. Production of a new TS document without existing documents to be based on (incl. stakeholder consultation). **Timescale** (planning): • Start: T0+6 • Complete: T0+24
19 174	TS	**Title: Signature Policy Testing Compliance & Interoperability**
		Description: Firstly this document 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.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: • Starting points: o Same as starting points for Signature Policies EN 19 172. • Other documents: o ETSI TS under production by ETSI TC ESI: "Conformity Testing for XAdES Baseline Profile" **(WI DTS/ESI-000095)**. o ETSI TS under production: "Test Suite for PDF Advanced Signatures (PAdES) interoperability test events" " **(WI DTS/ESI-000096)**. o ETSI TS under production: "Test Suite for Associated Signature Containers (ASiC) interoperability test events". (**WI DTS/ESI-000097)**. o Test suites for XAdES as developed for XAdES interoperability events. • Reasons why selecting starting points: The EN 19 172, is required for defining the complete set of conformity test suite as well as for defining adequate and test suites for interoperability tests. • Degree to which scope is met considering starting points: The current situation is different regarding the actual technical specification and whether conformity or interoperability testing is addressed. Details are provided below: o **Test suites for testing interoperability of signature policies. Little basis**. o **Specifications for testing compliance of signature policies. Little basis**.
		WORK PLAN **Task to be carried out**: Details are listed below regarding the different parts of the final TS**:** • **Test suites for testing interoperability for signature policies**. **Scope nearly met**. Production of a TS new document without existing documents to be based on (incl. stakeholder consultation). • **Specifications for testing compliance of signature policies**. Production of a new TS document based on a number of existing documents (incl. stakeholder consultation). **Timescale** (planning): • Start: T0+6 • Complete: T0+24

6.2.3 Signature Creation Devices

Summary

Table 9: Work Plan summary for Standards for Signature Creation and Other Related Devices

					Signature creation and other related devices	Degree scope met	Starting Points
					Sub-areas		
					Guidance		
TR	19	2	0	0	Business Driven Guidance for Signature Creation and Other Related Devices	Little basis	none
					Policy & Security Requirements		
EN	19	2	1	1	Protection Profiles for Secure Signature Creation Devices	Nearly met	EN 14169-1/6
EN	19	2	2	1	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures		
EN	19	2	3	1	Security requirements for trustworthy systems supporting time-stamping		
EN	19	2	4	1	Security Requirements for Trustworthy Systems supporting Server Signing (Signature Generation services)		
EN	19	2	5	1	Protection Profiles for Authentication Device		
					Technical Specifications		
EN	19	2	1	2	Application Interfaces for Secure Signature Creation Devices	Inputs exist	EN 14890
					Conformity Assessment		
EN	19	2	0	3	Conformity Assessment of Secure Devices and Trustworthy systems	Partially met	CWA 14172-5, 7
					Testing Compliance & Interoperability		
-	-	-	-	-	*no requirement identified*		

Details

Deliverable id	Type	Title and Contents
		GUIDANCE
19200	TR	**Title**: **Business Driven Guidance for Signature Creation Devices**
		Description: This document provides guidance for the selection of standards for electronic signature devices for given business requirements. This document needs to cover the following topics: • Need for electronic signatures • Background to the legislation • Summary of types of Signature (advanced and qualified) • Need for hardware to secure signature creation data • Discussion of personal versus corporate signatures. • Summary of the different protection profiles families: EN 19 211 for SSCD, EN 19 221 for other SCDs. **Suggestions for the work:** This informative in order to be useful needs to be short, and if possible with practical examples.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: none • Other documents: 19 000, 19 100, EN 19 211 for SSCD, EN 19 221, EN 19 231, EN 19 241, EN 19 251 for other signature related devices • Degree to which scope is met considering starting points: o Little basis
		WORK PLAN **Task to be carried out:** • Production of a new TR document based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 + 3 months • Complete: T0+12 A second review will be needed when all related EN will be ready.

Deliverable id	Type	Title and Contents
		POLICY & SECURITY REQUIREMENTS
19211	EN	**Title: Protection Profiles for Secure Signature Creation Devices**
		Description: This multi-part document specifies the security requirements for a SSCD. This includes security requirements on device with key generation and device with key import as well as security requirements for possible extensions. **Suggestions for the work:** One header document should be edited that points to the different parts of the ENs. The ENs should not be changed itself, because in this case a re-certification of the protection profiles needs to be performed.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: EN 14 169-1 to 6 • Other documents: - • Reasons why selecting starting points: • Currently, WG17 finalises EN 14 169-1, 2, 3, 4, 5, 6. Part 1 gives an overview and parts 2-6 will be certified as protection profiles (PP) for SSCDs. These certified PP can then be used in conformity assessment of SSCD products. No changes will be necessary to fit into the new structure of the rationalized framework as titles and scopes fit to the given definitions. • Degree to which scope is met considering starting points: o Scope: nearly met
		WORK PLAN **Task to be carried out:** Progression of an existing (proposed draft) EN to a full EN within Rationalised Framework classification **Timescale** (planning)**:** • Start: T0+2 • Complete: 2013 • Work could start after finalising the evaluation of the PPs and publication as ENs, scheduled for January 2013. **Task to be carried out:** • Additional study on the additional protection profiles or other form of security certification and security evaluation processes may be required, to ensure that they offer the relevant level of security, for other types of devices such as, e.g.: o Mobile phones with hardware- based security (TEE- MTM); o HSM being recognised as an SSCD; o SSCD used for mass signing operations. Possible delivery could be a work item description, if additional work is needed from the study. **Timescale** (planning)**:** • Start: T0 • Complete: T0+ 12
19221	EN	**Title: Security Requirements for trustworthy systems managing certificates for electronic signatures**
		Description: This multi-part document specifies the security requirements for TSPs. This includes security requirements on mandatory core functions (signing operations with or without backup, key generation) as well as security requirements for possible extensions. **Suggestions for the work:** One header document should be edited that points to the different parts of the ENs. The ENs should not be changed itself, because in this case a re-certification of the protection profiles needs to be performed.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 14 167-2, 3, 4, 5 • Other documents: - • Reasons why selecting starting points: Currently, WG17 updates CWA 14167-1,2,3,4 to technical specifications TS 14 167-1,2,3,4. Parts 2-4 will be certified as protection profiles (PP) for cryptographic modules. No (major) changes will be necessary to fit into the new structure of the rationalized framework as titles and scopes fit to the given definitions. It has been the intention to progress these to EN. • Degree to which scope is met considering starting points: o Scope nearly met
		WORK PLAN **Task to be carried out:** • Production of an EN from an existing document with updates **Timescale** (planning)**:** • Start: T0 • Complete: T0+2+18 Work could start after finalising the evaluation of the PPs and publication as TSs, scheduled for June 2012.
19231	EN	**Title: Security requirements for Trustworthy Systems supporting time-stamping**
		Description: This .document specifies security requirements for TSPs providing time-stamping services.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ANSSI PP-SH-CCv3.1 • Other documents: - • Reasons why selecting starting points: • Document matches the scope. • Degree to which scope is met considering starting points o Scope: partially met
		WORK PLAN **Task to be carried out:** • Production of PP • Evaluation/Certification of PP • Migration to EN **Timescale** (planning)**:** • Start: T0 • Complete: T0+ 24 +18
19241	EN	**Title: Security requirements for Trustworthy Systems supporting Server Signing (Signature Generation Services)**
		Description: This document specifies security requirements for trustworthy systems supporting signature generation services (server signing).
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 14167-5 • Other documents: - • Reasons why selecting starting points: Document matches the scope • Degree to which scope is met considering starting points: o Nearly met
		WORK PLAN **Task to be carried out:** • Production of TS Migration to EN document **Timescale** (planning)**:** • Start: T0 • Complete: T0+ 24+18

Deliverable id	Type	Title and Contents
19251	EN	**Title: Protection Profile for Authentication Device**
		Description: This multi-part document defines security requirements for conformity of authentication device from the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to a hardware device (such as, for example, a smart card or USB token) allowing its legitimate holder to authenticate himself when accessing an on-line service or to guarantee the origin authentication of data sent by the User to a distant agent.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: EN 16 248 • Other documents: - • Reasons why selecting starting points: Document matches the scope • Degree to which scope is met considering starting points: o Scope: nearly met
		WORK PLAN **Task to be carried out:** • Evaluation/Certification of PP • Publication as EN **Timescale** (planning)**:** • Start: T0 • Complete: T0+24+18
TECHNICAL SPECIFICATIONS		
19212	EN	**Title: Application Interface for SSCDs**
		Description: This document describes an application interface and behaviour of the SSCD in the context of identification, authentication and electronic signature services. **Suggestions for the work:** Complete the EN 14 890 series of standards by: • New part 1 as an introduction to the multi-part document. • Usage of electronic displays and keypads on card: Enhancement of parts 2 and 3 regarding the usage of these devices. • Web services on card, including first networking and middleware on card aspects, second enhancement of Part 2 regarding signature creation and verification for applications API-based, third enhancement of Part 3 regarding C/S authentication (end-to-end security), with respect to ETSI format for signatures fourth a glossary including the unambiguous definition of the security properties employed by the described protocols A. • New part 4 describing context specific authentication protocols for SSCDs, covering first the migration to suitable Authentication Protocols e.g. for further context specific use for other transport layers e.g. NFC, and second a glossary including the unambiguous definition of the security properties employed by the proposed protocols. One scenario is the usage of a contactless card as SSCD with a mobile device such as a mobile phone or tablet as SCA. In this case the display and keypad of the mobile device which are secured by a Trusted Execution Environment (TEE) are used as secure display resp. keypad and the new part 4 standardises the authentication protocols between the SSCD and the mobile device. • EN 19 212 will reference TS 19 312 for guidance on cryptographic algorithms.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: EN 14 890-1/2 • Other documents: - • Reasons why selecting starting points: Most relevant document. • Degree to which scope is met considering starting points (choice): o Input exists

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out:** • Significant revision to an existing document **Timescale** (planning)**:** • Start: T0 • Complete: T0+24+18
CONFORMITY ASSESSMENT		
19203	EN	**Title: Conformity Assessment of Secure Devices and Trustworthy Systems**
		Description: This document specifies requirements for conformity assessment of Secure Signature Creation Devices and other device and trustworthy systems for electronic signatures and related services. It will make reference to the relevant common criteria evaluation, or other, methodologies and describe any specific requirements for evaluation against the standard protection profiles or security requirements document.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: CWA 14172-5 & CWA 14172-7 • Other documents: Common Criteria for Information Technology Security Evaluation • Reasons why selecting starting points: There is no update planned by the WG17 on CWA 14172-5, 7 so there is a need to transform it to EN, and complete the scope (current version is from 2004). • Degree to which scope is met considering starting points (choice): o Scope partially met
		WORK PLAN **Task to be carried out:** • Significant revision to an existing document (before progression to EN) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12+18 The work could start in Q2 2012.

6.2.4 Cryptographic Suites

Summary

Table 10: Work Plan summary for Standards for Cryptographic Suites

						Cryptographic Suites	Degree scope met	Starting Points
						Sub-areas		
						Guidance		
TR	19	3	0	0		Business Driven Guidance for Cryptographic Suites	Little basis	none
						Technical Specifications		
TS	19	3	1	2		Cryptographic Suites for Secure Electronic Signatures	Partially met	TS 102176
						Testing Compliance & Interoperability		
-	-	-	-	-		*no requirement identified*		

Details

Deliverable id	Type	Title and Contents
		GUIDANCE
19300	TR	**Title: Business Driven Guidance for Cryptographic Suites**
		Description: This document provides guidance for the selection of cryptographic suites for given business requirements. Interoperability of eSignature within Europe matters. Security requirements differ from one country to another. Therefore it is necessary to define what is mandated to address security requirements in various business cases. These business cases deal with the different components, devices and applications, used in the context of electronic signature. **Suggestions for the work:** This document is linked to TS 19 312.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: none • Other documents: 19 000 and 19 100 • Reasons why selecting starting points • Degree to which scope is met considering starting points: o Little basis
		WORK PLAN **Task to be carried out:** (choice) • Production of a new document (TR) without existing documents to be based on (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 + 3 • Complete: T0 + 12
		TECHNICAL SPECIFICATIONS
19312	TS	**Title: Cryptographic Suites for Secure Electronic Signature**
		Description: 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. **Suggestions for the work:** • To ensure a proper use and implementation of this document, it should be clearly indicated and referred in the other TR, TS or EN related to electronic signature. • This document should be a subset of all existing national catalogues to guarantee compliance with national laws and national evaluation bodies' recommendations. The working group should be formed by cryptographic experts from various countries where cryptographic recommendations are expressed, at least France (ANSSI Référentiel Général de Sécurité) and Germany (BSI catalogue). National bodies including at least France (ANSSI) and Germany (BSI) should be involved by direct participation or consultation). SOGIS should be involved or consulted for review before publication. • Coordination with CEN TC224 WG16 should be active. • Regular maintenance of this document should be ensured by ETSI ESI on a yearly basis, within a group formed following above recommendations.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 102 176 • Other documents: French Référentiel Général de Sécurité, German catalog, American National Institute for Standards and Technology, academic studies (e.g. ECRYPT II), keylengths.org • Reasons why selecting starting points: TS 102 176 is the former description of cryptographic suites for secure electronic signatures • Degree to which scope is met considering starting points: o Scope partially met

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out:** • Significant revision to an existing document (but no progression to EN) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12 months

NOTE: SOGIS is the Senior Officials Group – Information Systems Security which is a body of the European Commission. This group has signed a Mutual Recognition Agreement to recognise certificates on IT-Security evaluation from other countries. The SOGIS Mutual Recognition Agreement is an agreement to recognise Common Criteria certificates of other countries for all Evaluation Assurance Levels (EAL1 up to EAL7).

6.2.5 TSP Supporting Electronic Signatures

Summary

Table 11: Work Plan summary for Standards for TSP supporting Electronic Signatures

						TSPs Supporting Electronic Signatures and related services	Degree scope met	Starting Points
						Sub-areas		
						Guidance		
TR	19	4	0	0		Business Driven Guidance for TSPs Supporting Electronic Signatures	Little basis	
						Policy & Security Requirements		
EN	19	4	0	1		General Policy Requirements for TSPs Supporting Electronic Signatures	Nearly met	DEN/ESI 000117
EN	19	4	1	1		Policy & Security Requirements for TSPs Issuing Certificates	Partially met	TS 101 456/102 042 + CAB Guidelines
						Part 1: Overview		TS 102 158
						Part 2: Policy requirements for TSP issuing QCs		
						Part 3: Policy requirements for TSPs issuing PKCs		
						Part 4: Policy requirements for TSP issuing SSL EV Certificates		
						Part 5: Policy requirements for TSP issuing SSL Baseline Certificates		
						Part 6: Policy requirements for TSP issuing Attributes Certificates		
EN	19	4	2	1		Policy & Security Requirements for TSPs providing Time-Stamping Services	Partially met	TS 102 023
						- Part 1: Overview		
						- Part 2: Policy requirements for TSPs providing Time-Stamping Services		
EN	19	4	3	1		Policy & Security Requirements for TSPs providing Signature Generation Services	Inputs exist	
						- Part 1: Overview		
						- Part 2: Policy requirements for TSPs providing Signature Generation Services		
EN	19	4	4	1		Policy & Security Requirements for TSPs providing Signature Validation Services	Inputs exist	
						- Part 1: Overview		
						- Part 2: Policy requirements for TSPs providing Signature Validation Services		
						Technical Specifications		
EN	19	4	1	2		Profiles for TSPs issuing Certificates	Partially met	TS 101 862 / 102 280
						- Part 1: Overview		
						- Part 2: Certificate profile for certificates issued to Natural persons (TS 102 280)		
						- Part 3: Certificate profile for certificates issued to legal persons		
						- Part 4: Profiles SSL/TSL certificates issued to organisation (Baseline & EV)		
						- Part 5: Extensions for Qualified Certificate Profile (pre-EN 301 862)		
EN	19	4	2	2		Profiles for TSPs providing Time-Stamping services	Nearly met	TS 102 861
EN	19	4	3	2		Profiles for TSPs providing Signature Generation Services	Inputs exist	
EN	19	4	4	2		Profiles for TSPs providing Signature Validation Services	Inputs exist	
						Conformity Assessment		
EN	19	4	0	3		General requirements and guidance for Conformity Assessment of TSPs supporting e-Signatures	Nearly met	DTS/ESI-000075
EN	19	4	1	3		Conformity Assessment for TSPs Issuing Certificates	Partially met	DTS/ESI-000075
						- Part 1: Conformity Assessment for Policy requirements for TSPs issuing Certificates		
						- Part 2: Conformity Assessment for Profiles for TSPs issuing Certificates		
EN	19	4	2	3		Conformity Assessment for TSP providing time-stamping services	Partially met	DTS/ESI-000075 CWA 141
						- Part 1: Conformity Assessment for Policy requirements for TSPs providing time-stamping services		
						- Part 2: Conformity Assessment for Profiles for TSP providing time-stamping services		
EN	19	4	3	3		Conformity Assessment for TSPs providing Signature Generation Services	Little basis	
EN	19	4	4	3		Conformity Assessment for TSPs providing Signature Validation Services	Little basis	
						Testing Compliance & Interoperability		
-	-	-	-	-		*no requirement identified for such a document*		

Details

Deliverable id	Type	Details, Analysis and Work Plan
		GUIDANCE
19 400	**TR**	**Title: Business Driven Guidance for TSPs Supporting Electronic Signatures**
		Description: This document provides guidance for the selection of standards for TSPs for given business requirements. This will build on the guidance from the viewpoint of signature creation and validation providing further guidance on the selection of standards and options from the viewpoint of TSPs supporting electronic signatures
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: none • Reasons for selecting starting point: This guidance refines the guidance for signature creation and validation from the viewpoint of the TSP • Other documents: 19 000 and 19 100 • Degree to which scope is met: o Little basis
		WORK PLAN **Task to be carried out:** • Production of a new TR without existing documents to be based on TR 19 100 (incl. stakeholder consultation) **Timescale:** • Start: T0 + 3 months • Complete: T0 + 12 Months
		POLICY AND SECURITY REQUIREMENTS
19 401	**EN**	**Title: General Policy Requirements for TSPs Supporting Electronic Signatures**
		Description: This document specifies policy requirements for TSPs Supporting Electronic Signatures that are independent of the type of TSP.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: • Starting points: ETSI Quick Fix on general policy requirements (DEN/ESI-000117) • Reasons for selecting starting point: Document matches the scope extracting general requirements from TS 101 456 and TS 102 042. • Degree to which scope is met: o Scope nearly met
		WORK PLAN **Task to be carried out:** • Progression of an existing (proposed draft) EN to a full EN within Rationalised Framework classification **Timescale:** • Start: Ongoing quick fix activity • Complete: Q1 2013
19 411	**EN**	**Title: Policy & Security Requirements for TSPs Issuing Certificates**
		This (multi-part) document specifies policy and security requirements for TSPs issuing certificates. It references EN 19 401 for generic requirements. This is a multi-part document including the following topics: • Overview: This part provides an overview of the other parts of this document. It also describes the relationship of the policy requirements defined in this area and the use of secure devices and trustworthy systems defined in the "Signature Creation and Other Related Device" area. • Policy requirements for TSP issuing QCs. • Policy requirements for TSP issuing public key certificates (other than qualified certificates). • Policy requirements for TSP issuing SSL Extended Validation certificates. • Policy requirements for TSP issuing SSL baseline certificates. • Policy requirements for TSP issuing Attribute Certificates. Informative annexes will provide check lists for conformity assessment.

Deliverable id	Type	Details, Analysis and Work Plan
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: o Overview: none o Policy requirements ETSI Quick Fix, prEN 101 456 & prEN 102 042 o CAB Forum document DTR-ESI-0000107 • Reasons for selecting starting point: Document matches the scope • Degree to which scope is met: o Scope partially met
		WORK PLAN **Task to be carried out:** • Production of overview document (joint CEN and ETSI activity) • Progression of part 2 and 3 to EN including take account of implications of using signature generation services. • Production of policy requirements sub-parts (ETSI) for SSL and attributes certificates • Production of annexes providing conformity checklists **Timescale:** • Start: T0 (some activities ongoing quick fix activity) • Complete: T0 + 24
19 421	**EN**	**Title: Policy & Security Requirements for TSPs providing Time-Stamping Services**
		Description: This document specifies policy requirements for TSPs providing Time-stamping services based on RFC 3161 [i.16]. It is to be a multi part document including: • Overview • Policy requirements for TSP providing Time-stamping referencing EN 19 401 for general requirements
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: o Overview: none o Policy requirements ETSI TS 102 023 • Reasons for selecting starting point: Document matches the scope. • Degree to which scope is met: o Scope partially met
		WORK PLAN **Task to be carried out:** • Production of overview document (joint CEN and ETSI activity) • Progression of TS 102 042 to EN (ETSI) • Production of annexes providing conformity checklists **Timescale:** • Start: T0 • Complete: T0 + 24 Months
19 431	**EN**	**Title: Policy Requirements for TSPs providing Signature Generation Services**
		Description: This document specifies policy requirements for TSPs providing signature generation services. It is to be a multi part document including: • Overview • Policy requirements for TSP providing signature generation referencing EN 19 401 for general requirements
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: None identified • Reasons for selecting starting point: N/A • Degree to which scope is met: o Inputs exist (19 401)

Deliverable id	Type	Details, Analysis and Work Plan
		WORK PLAN **Task to be carried out:** • Production of overview document (joint CEN and ETSI activity) • Production of policy requirements (ETSI) • Production of annex providing conformity checklists **Timescale:** • Start: T0 • Complete: T0 + 24 months
19 441	**EN**	**Title: Policy Requirements for TSPs providing Signature Validation Services**
		Description: This document specifies policy requirements for TSPs providing signature validation services. It is to be a multi part document including: • Overview • Policy requirements for TSP providing signature validation referencing EN 19 401 for general requirements • Production of annex providing conformity checklists
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: None identified • Reasons for selecting starting point • Degree to which scope is met: o Inputs exist (19 401)
		WORK PLAN **Task to be carried out:** • Production of overview document (joint CEN and ETSI activity) • Production of policy requirements (ETSI) • Production of annex providing conformity checklists **Timescale:** • Start: T0 • Complete: T0 + 24 months
TECHNICAL SPECIFICATIONS		
19 412	**EN**	**Title: Profiles for TSPs issuing Certificates**
		Description: This document provides specifications for specific profiles applicable to TSPs issuing certificates. It is a multi-part document including the following parts: • Overview • Certificate profile for certificates issued to natural persons (based on TS 102 280) • Certificate profile for certificates issued to legal persons • Profiles for SSL/TSL Certificates issued to organisation (Baseline and Extended Validation) • Extensions for Qualified Certificate Profile (based on pre-EN 301 862)
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: o ETSI Quick Fix prEN 301 862 o ETSI Quick Fix Revised TS 102 280 o CAB Forum requirements • Reasons for selecting starting point: Document matches the scope • Degree to which scope is met: o Scope partially met

Deliverable id	Type	Details, Analysis and Work Plan
		WORK PLAN **Task to be carried out:** • Production of new part 1 (overview) • Update to part 2 taking into account TS 102 280 • Production of new part 3 (legal persons) based on part 2 • Production of new part 4 based on ETSI work on CAB Forum Guidelines and TS 102 042. • Progression of Part 5 to EN from pre-EN 301 862 **Timescale:** • Start: T0 • Complete: T0 + 24 Months
19 422	**EN**	**Title: Profiles for TSPs providing Time-Stamping Services**
		Description: This document specifies a profile for the format and procedures for time-stamping as specified in RFC 3161 [i.16].
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 101 861 • Reasons for selecting starting point: Document matches the scope • Degree to which scope is met: o Scope nearly met
		WORK PLAN **Task to be carried out:** • Production of an EN from an existing document with minor updates **Timescale:** • Start: T0 • Complete: T0 + 18 Months
19 432	**EN**	**Title: Profiles for TSPs providing Signature Generation Services**
		Description: This document specifies a profile for the format and procedures for TSPs providing Signature Generation Services.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: OASIS DSS, Austrian MOA-SS/SP, ETSI TS 102 206 • Reasons for selecting starting point: Similar server based solutions to providing signing services, particular for mobile devices. • Degree to which scope is met: o Inputs exist
		WORK PLAN **Task to be carried out:** • Production of a new document (e.g. EN, TS) based on a number of existing documents (incl. stakeholder consultation) **Timescale:** • Start: T0 • Complete: T0 + 24 Months
19 442	**EN**	**Title: Profiles for TSPs providing Signature Validation Services**
		Description: This document specifies a profile for the format and procedures for TSPs providing Signature Validation Services.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: OASIS DSS, Austrian MOA-SS/SP • Reasons for selecting starting point: • Degree to which scope is met: o Inputs exist

Deliverable id	Type	Details, Analysis and Work Plan
		WORK PLAN **Task to be carried out:** • Production of a new document (e.g. EN, TS) based on a number of existing documents (incl. stakeholder consultation) **Timescale:** • Start: T0 • Complete: T0 + 24 Months
CONFORMITY ASSESSMENT		
19 403	**EN**	**Title: General requirements and guidance for Conformity Assessment of TSPs Supporting Electronic Signatures**
		Description: This document specifies general requirements for conformity assessment independent of the form of TSP
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: • Starting points: ETSI Quick fix on CSP Conformity Assessment DTS/ESI-000075 • Reasons for selecting starting point: Matches scope • Degree to which scope is met: o Scope nearly met
		WORK PLAN **Task to be carried out:** • Production of an EN from an existing document with minor updates. Further consultation with stakeholders required to ensure consensus. **Timescale:** • Start: T0 • Complete: T0 + 24 Months
19 413	**EN**	**Title: Conformity Assessment for TSPs Issuing Certificates**
		Description: This document specifies requirements for the conformity assessment of a Certification Authority issuing public key certificates including qualified certificates.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI Quick fix on CSP Conformity Assessment DTS/ESI-000075, CWA 14172-3 • Reasons for selecting starting point: Provides common basis for conformity assessment • Degree to which scope is met: o Scope partially met
		WORK PLAN **Task to be carried out:** • Production of conformity assessment document on policy requirements (ETSI) **Timescale:** • Start: T0 • Complete: T0 + 24 Months
19 423	**EN**	**Title: Conformity Assessment for TSPs providing Time-Stamping Services**
		Description: This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing time-stamping services.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI Quick fix on CSP Conformity Assessment DTS/ESI-000075, CWA 14172-8 • Reasons for selecting starting point: Provides common basis for conformity assessment • Degree to which scope is met: o Scope partially met

Deliverable id	Type	Details, Analysis and Work Plan
		WORK PLAN **Task to be carried out:** • Production of conformity assessment document on policy requirements (ETSI) **Timescale:** • Start: T0 • Complete: T0 + 24 Months
19 433	**EN**	**Title: Conformity Assessment for TSPs providing Signature Generation Services**
		Description: This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing signature generation services.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI Quick fix on CSP Conformity Assessment DTS/ESI-000075, CWA 14172-7 • Reasons for selecting starting point: Provides common basis for conformity assessment • Degree to which scope is met: o Little basis
		WORK PLAN **Task to be carried out:** • Production of conformity assessment document on policy requirements (ETSI) **Timescale:** • Start: T0 • Complete: T0 + 24 Months
19 443	**EN**	**Title: Conformity Assessment for TSPs providing Signature Validation Services**
		Description: This document specifies requirements and provides guidance for the supervision and assessment of a TSP providing signature validation services.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI Quick fix on CSP Conformity Assessment DTS/ESI-000075, CWA 14172-4 • Reasons for selecting starting point: Provides common basis for conformity assessment • Degree to which scope is met: o Scope partially met
		WORK PLAN **Task to be carried out:** • Production of conformity assessment document on policy requirements (ETSI) **Timescale:** • Start: T0 • Complete: T0 + 24 Months

6.2.6 Trust Application Service Providers

Summary

Table 12: Work Plan summary for Standards for Trust Application Service Providers

					Trust Application Service Providers	Degree scope met	Starting Points	Complete by
					Sub-areas			
					Guidance			
TR	19	5	0	0	Business Driven Guidance for Trust Application Service Providers	Little basis	none	T0+12
SR	19	5	3	0	Study on standardisation requirements for e-Delivery services applying e-Signatures	Inputs exist	See description	T0+12
					Policy & Security Requirements			
EN	19	5	1	1	Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers	Inputs exist	TS 102640-3/4	T0+24
EN	19	5	2	1	Policy & Security Requirements for Data Preservation Service Providers (DPSPs)	partially met	TS 101533-1	T0+18
					Technical Specifications			
EN	19	5	1	2	Registered Electronic Mail (REM) Services	Scope fully met	TS 102640-1,2,5,6	T0+12
EN	19	5	2	2	Data Preservation Services through signing	Inputs exist	TS 101533-1	T0+24
					Conformity Assessment			
EN	19	5	1	3	Conformity Assessment for REM Service Providers	Inputs exist	TS 102640-4	T0+24
SR	19	5	2	3	Conformity Assessment of Data Preservation Service Providers	Inputs exist	TS 101533-2	T0+12
					Testing Compliance & Interoperability			
TS	19	5	0	4	General requirements for Testing Compliance & Interoperability of TASPs	Inputs exist	none	T0+12
TS	19	5	1	4	Testing Compliance & Interoperability of REM Service Providers	Inputs exist	TS 102640-6	T0+12

Details

Deliverable id	Type	Title and Contents
		GUIDANCE
19 500	TR	**Title: Guidance for Trust Application Service Provider**
		Description: 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.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: None • Degree to which scope is met considering starting points: o Little basis
		WORK PLAN **Task to be carried out:** • Production of a new TR document without existing documents to be based on (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12

Deliverable id	Type	Title and Contents
19 530	SR	**Title: Study into standardisation requirements for Electronic Delivery Applying Electronic Signatures**
		Description: This SR will define Electronic Delivery (e-delivery) services and investigate applicable requirements from those existing in the market (ETSI, CEN, private standards and pilots' outcome) proposing rationalised and well organized requirements for Electronic Delivery Applying Electronic Signatures and its possible relation to Registered E-Mail. E-delivery services, in addition to deliver data objects to purported recipients, should be also able 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. Early in 2006, ETSI identified an increasing need across Europe for a trustable electronic mail system, suitable to exchange electronic messages with a similar reliability to paper Registered Mail, i.e. systems able to generate trusted electronic evidence attesting that certain events had taken place (submission by a sender of a message to a recipient, delivery of the message to the recipient, etc.). By that time, there were already implementations at national level within a number of European countries (like Posta Elettronica Certificata in Italy, De-mail and EGVP in Germany, IncaMail in Switzerland), and even legislation providing legal value to the evidence set generated by such kind of systems. ETSI delivered in January 2010 the ETSI Technical Specification (TS) 102 640 on "Registered Electronic Mail (REM)", a document to enable implementations of REM systems issuance of reliable evidence endorsed by relevant legislation, which was reviewed in September 2011 to help interoperability with REM-like systems based on SMTP and with some pilots on so-called e-delivery. The Universal Postal Union (UPU) has also developed a SOAP-based mailing system and the European Commission has supported and funded a number of very relevant Large Scale European Projects, which had to deal in one way or the other, with the reliable exchange of electronic documents between different parties in different contexts: • PEPPOL (Pan-European Public eProcurement On-Line) • SPOCS (Simple Procedures Online for Cross-border Services) • STORK (Secure identity across borders linked) being the most relevant, and • E-CODEX (e-Justice Communication via Online Data Exchange), among others All this Large Scale European Projects had decided to use SOAP on HTTP as the technical means for implementing such an exchange, which lead to conclude that SOAP based systems will in the future likely affect most of the European Member State Public Administrations and, in a time lapse that is still difficult to foresee, possibly nearly all the postal authorities at the global level. In view of the multiplicity of approaches and projects on this matter, it appears as advisable to conduct a Study on e-delivery requirements and definition in order to propose a rationalise set of standards that fulfil the gap among the different standardizations efforts and pilots' outcome documentation.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: none • Other documents: TS 102 640-3 V2.1.2 (2011-05) Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 3: Information Security Policy Requirements for REM Management Domains; TS 102 640-4 Registered Electronic Mail (REM): Architecture, Formats and Policies - Part 4: REM-MD Conformance Profiles; and relevant documents and outcomes from SPOCS, PEPPOL, e-CODEX and UPU SOAP-based mailing system specifications. • Reasons why selecting starting points: Relevant input. • Degree to which scope is met considering starting points: o Input exists
		WORK PLAN **Task to be carried out:** • Production of a SR based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12

Deliverable id	Type	Title and Contents
		POLICY AND SECURITY REQUIREMENTS
19 511	EN	**Title: Policy & Security Requirements for Registered Electronic Mail (REM) Service Providers**
		Description: This document specifies policy requirements for REM 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 19 502). It references EN 19 501 for generic requirement.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 102 640-3 V2.1.2 (2011-05) Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 3: Information Security Policy Requirements for REM Management Domains; TS 102 640-4 Registered Electronic Mail (REM): Architecture, Formats and Policies - Part 4: REM-MD Conformance Profiles • Reasons why selecting starting points: These documents includes security requirements of REM services • Degree to which scope is met considering starting points: o Input exists
		WORK PLAN **Task to be carried out:** • Production of a new document (e.g. EN, TS) based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12+12
19 521	EN	**Title: Policy & Security Requirements for Data Preservation Service Providers (IPSPs)**
		Description: This document specifies policy requirements for DPSPs. It references EN 19 501 for generic requirements. This document also references the Security requirements for TASP trustworthy systems (EN 19 502) and may address specific Information Security Management Systems or Data Preservation Systems, by specifying specific security requirements for Data Preservation Service Providers to abide by, when implementing and managing a DPS, in order to provide Data 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.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 101 533-01 Data Preservation Systems Security- Part 1: Requirements for Implementation and Management • Reasons why selecting starting points: This document set out DPSP security and policy requirements • Degree to which scope is met considering starting points: o Scope partially met
		WORK PLAN **Task to be carried out:** • Production of a new EN document based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+6+12

Deliverable id	Type	Title and Contents
		TECHNICAL SPECIFICATION
19 512	EN	**Title: Registered Electronic Mail Services**
		Description: This document provides technical specifications for the provision of Registered Electronic Mail. 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 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: Its internal structure will very much depend on the different relevant systems specified and built across Europe, as during the last years a number of specifications and non interoperable systems based on them, have been developed.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 102 640-1 Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 1: Architecture; TS 102 640-2 Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 2: Data requirements, Formats and Signatures for REM. • ETSI TS 102 640-5 Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 5: REM-MD Interoperability Profiles. • ETSI TS 102 640-6 Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 6: "Interoperability Profiles". • Reasons why selecting starting points: These documents cover the scope. • Degree to which scope is met considering starting points: o Scope fully met

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out:** • Production of an EN from an existing document with minor updates **Timescale** (planning): • Start: T0 • Complete: T0+12
19 522	EN	**Title: Information Preservation Services through signing**
		Description: 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.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 101 533-01 Information Preservation Systems Security- Part 1: Requirements for Implementation and Management • Reasons why selecting starting points: Some signatures features are present in that document • Degree to which scope is met considering starting points: o Input exists
		WORK PLAN **Task to be carried out**: • Initially a study is to be carried out on any standardisation requirements in this area, and how this relates to general standards for archiving and electronic signatures. **Timescale** (planning): • Start: T0 • Complete: T0+12
		CONFORMITY ASSESMENT
19 513	EN	**Title: Conformity Assessment of Registered Electronic Mail Service Providers**
		Description: This document specifies requirements and provides guidance for the supervision and assessment of a Registered Electronic Mail Service Provider. This document will provide a common set of criteria to assess implemented security and policy requirements against EN 19 511, usable by assessors.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 102 640-4 Registered Electronic Mail (REM): Architecture, Formats and Policies - Part 4: REM-MD Conformance Profiles • Other documents: ISO 17011, EN 45011, ISO 17021, ISO 17065 • Reasons why selecting starting points: Some information on conformance profile • Degree to which scope is met considering starting points: o Inputs exist
		WORK PLAN **Task to be carried out:** • Production of a new EN document based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12+12
19 523	EN	**Title: Conformance Assessment of Data Preservation Service Providers**
		Description: This document specifies requirements and provides guidance for the supervision and assessment of a DPSP. This document will provide a common set of criteria to review implemented security and policy requirements as per EN 19 521, usable by assessors of Data Preservation Systems.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TR 101 533-02 Data Preservation Systems Security-Part 2: Guidelines for Assessors • Other documents: ISO 27001, ISO 27002, ISO 27007

Deliverable id	Type	Title and Contents
		• Reasons why selecting starting points: This document provides some inputs on assessors guidelines: o Degree to which scope is met considering starting points: Input exists
		WORK PLAN **Task to be carried out:** • Production of a new EN document based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12+12
TESTING COMPLIANCE & INTEROPERABILITY		
19 504	TS	**Title: General requirements for Technical Conformity & Interoperability Testing for Trust Application Service Providers**
		Description: This document specifies general requirements for specifying technical conformity and interoperability testing for TASPs.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI TR 103 071 Test suite for future REM interoperability test events • Degree to which scope is met considering starting points: o Inputs exist
		WORK PLAN **Task to be carried out:** • Production of a new TS document based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12
19 514	TS	**Title: Testing Compliance & Interoperability of Registered Electronic Mail and Service Providers**
		Description: 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. • Testing compliance: This document specifies the tests to be performed for checking conformance against EN 19 512. 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.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: ETSI TR 103 071Test suite for future REM interoperability test events; ETSI TS 102 640-6 Registered Electronic Mail (REM); Architecture, Formats and Policies- Part 6: "Interoperability Profiles". • Degree to which scope is met considering starting points: o Input exists

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out:** • Production of a new TS document based on a number of existing documents (incl. stakeholder consultation) **Timescale** (planning)**:** • Start: T0 • Complete: T0+12

6.2.7 Trust Service Status List Providers

Summary

Table 13: Work Plan summary for Standards for Trust Service Status Lists Providers

						Trust Service Status Lists Providers	Degree scope met	Starting Points
						Sub-areas		
						Guidance		
TR	19	6	0		0	Business Driven Guidance for Trust Service Status Lists Providers	Little basis	
						Policy & Security Requirements		
EN	19	6	0		1	General Policy & Security Requirements for Trust Service Status Lists Providers (TSSLPs)	Inputs exist	
EN	19	6	1		1	Policy & Security Requirements for Trusted Lists Providers	Inputs exist	
						Technical Specifications		
EN	19	6	0		2	Trust Service Status Lists Format	Nearly met	TS 102 231
EN	19	6	1		2	Trusted Lists Format	Nearly met	TS 102 232, CD
						Conformity Assessment		
EN	19	6	0		3	General requirements and guidance for Conformity Assessment of TSSLPs	Inputs exist	none
EN	19	6	1		3	Conformity Assessment of Trusted List Providers	Inputs exist	none
						Testing Compliance & Interoperability		
TS	19	6	0		4	General requirements for Testing Compliance & Interoperability of TSSLPs	Inputs exist	TSL PlugTest
TS	19	6	1		4	Testing Compliance & Interoperability of Trusted Lists	Nearly met	TSL PlugTest

Details

Deliverable id	Type	Title and Contents
		GUIDANCE
19600	TR	**TITLE: Business Driven Guidance for Trust Service Status Lists Providers**
		CONTENT: This document provides guidance for the selection of standards for Trusted Service Status Lists Providers for given business requirements. This document needs to cover the following topics: • Definition of *Trust* • Need for *Trust Anchors* • Distribution of *Trust Anchors* • Role of Trust Status Providers • Role of Trusted Lists • Selection of Standards to implement Trust Status Provisioning
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: None • Other documents: 19 000 and 19 100, TS 102 231 • Degree to which scope is met considering starting points: ○ Little basis
		WORK PLAN: **Task to be carried out:** • Production of a new document (TR) **Timescale** (planning)**:** • Start: T0 +3 • Complete: T0+12

Deliverable id	Type	Title and Contents
		POLICY & SECURITY REQUIREMENTS
19601	**EN**	**Title: General Policy & Security Requirements for Trust Service Status Lists Providers**
		Description: This document specifies general policy requirements for providers issuing status information of trusted services. This document needs to cover the following topics: • Legal requirements for Trust Service Status Providers • Policy requirements specific to Trust Service Status Providers • Design requirements for Trust Service Status Providers • Implementation requirements for Trust Service Status Providers
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** Currently no documents of this kind exist. Since the reliability and Security of Trust Service Status Providers has to be at least as high as for any of the trust services it services, this document will build on document 19101, being more specific in aspects especially relevant for trust service provisioning. • Starting points: None • Other documents: TS 102 231, **19 401** • Degree to which scope is met considering starting points: o Inputs exist
		WORK PLAN **Task to be carried out:** • Production of a new document (EN) based on a number on other policy requirements documents **Timescale** (planning)**:** • Start: T0 • Complete: T0+24
19611	EN	**Title: Policy & Security Requirements for Trusted Lists Providers**
		Content: 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].
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** This document will be based on EN 19601, but will specifically consider Trusted Lists as they are defined in CD 2009/767/EC [i.19] as amended by CD 2010/425/EU [i.20]. It will profile the base document to define a subset of requirements that is specific to that implementation of trust service provisioning. • Starting points: None • Other documents: TS 102 231, **19 401, 19 601** • Degree to which scope is met considering starting points: o Inputs exist
		WORK PLAN **Task to be carried out:** • Production of a new document (EN) based on a number of existing documents **Timescale** (planning)**:** • Start: T0 • Complete: T0+24
		TECHNICAL SPECIFICATIONS
19602	EN	**Title: Trust Service Status Information Formats**
		Description: 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) covering ASN.1, XML as well as human readable formats for TSLs. It will build on existing specifications (TS 102 231) and take experiences from Plugtests and experiences of current deployment into account.

Deliverable id	Type	Title and Contents
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 102 231 • Other documents: none. • Degree to which scope is met considering starting points: o Nearly met
		WORK PLAN **Task to be carried out** • Production of a new EN document based on an existing documents **Timescale** (planning): • Start: T0 • Complete: T0+6+12
19612	EN	**Title: Trusted Lists**
		Description: This document contains all the specifications related to Trusted Lists as they are defined in CD 2009/767/EC [i.19] amended by CD 2010/425/EU [i.20].
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 102 231, CD 2009/767/EC, CD 2010/425/EU • Other documents: 19 602 • Degree to which scope is met considering starting points: o Nearly met
		WORK PLAN **Task to be carried out:** • Production of a new EN document based on a number of existing documents **Timescale** (planning)**:** • Start: T0 • Complete: T0+6+12
To be decided		**Title: Study on Usage procedures of Trust Service Status Lists**
		Description: Investigate standardisation requirements to address the needs to specify the usage procedures of TSL (Trust Service Status List) and in particular to study implications of applying TSL and TL (Trusted List) to signature validation, taking into account legal and liability issues, and make recommendations on necessary updates to specifications potentially including, signature validation, TSL, TL, signature policies and conformity assessment.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: TS 102 231, CD 2009/767/EC, CD 2010/425/EU and • Other documents: 19 102 • Inputs exist
		WORK PLAN **Task to be carried out:** • Produce Study report on usage procedures of TSL and TL and recommendations regarding change requests to standards. **Timescale** (planning)**:** • Start: T0 • Complete: T0+6
CONFORMITY ASSESSMENT		
19603	EN	**Title: General requirements and guidance for Conformity Assessment of TSSLPs**
		Description: This document provides the rationale, rules and guidance on conformity assessment concerning the processes and products around the issuance and processing of Trust Service Status Lists.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting points: none • Other documents: 19 403 • Degree to which scope is met considering starting points: o Inputs exist

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out:** • Production of a new EN based around the general requirements specified in 19 403 **Timescale** (planning)**:** • Start: T0+3 • Complete: T0+3+24
19613	EN	**Title: Conformity Assessment of Trusted Lists Providers**
		Content: This document specifies the specific conformity rules for assessing conformity against EN 19 612 specifications related to both their generation and verification.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** • Starting point: none • Other documents:19 403. • Degree to which scope is met considering starting points: o Inputs exist
		WORK PLAN **Task to be carried out:** • Production of a new EN based around the general requirements specified in 19 403 **Timescale** (planning)**:** • Start: T0+3 • Complete: T0+3+24
TESTING COMPLIANCE & INTEROPERABILITY		
19604	TS	**Title: General requirements for Testing Compliance & Interoperability of TSSLPs**
		Description: This document specifies general requirements for specifying technical compliance and interoperability testing for TSSLPs.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis**: No formal document exists, but experiences with testing Trusted Lists as they are defined in CD 2009/767/EC [i.19] as amended by CD 2010/425/EU [i.20], the existing Portal for Electronic Signatures provide a sound basis for writing such a document. • Starting points: TSL PlugTests specifications • Other documents: none. • Degree to which scope is met considering starting points: o Inputs exist
		WORK PLAN **Task to be carried out:** • Production of a new TS document based on existing documents **Timescale** (planning)**:** • Start: T0 Complete: T0+12
19614	TS	**Title: Test suites and tests specifications for Technical Conformity & Interoperability Testing of Trusted Lists**
		Description: This document provides technical specifications for helping implementers and accelerating the development of tools for creating and issuing Trusted Lists.
		ANALYSIS: **Relevant inputs from Inventory (starting points) as a result from Analysis:** No formal document exists, but experiences with testing Trusted Lists as they are defined in CD 2009/767/EC [i.19] as amended by CD 2010/425/EU [i.20], the existing Portal for Electronic Signatures provide a "nearly met" basis for writing such a document: • Starting points: TSL PlugTests specifications • Other documents: none • Degree to which scope is met considering starting points: o Nearly met

Deliverable id	Type	Title and Contents
		WORK PLAN **Task to be carried out:** • Production of a new TS document based on existing documents **Timescale** (planning)**:** • Start: T0 • Complete: T0+6

6.3 General Conclusions

With regards to the work plan timescale, T0 is used as being the effective start of Phase 2 activities (after specialist task forces/project teams have been set up by CEN/ETSI). For the purpose of the consolidated figure below, the currently estimated T0 is September 2012. Prior to T0 there is expected to be a 3 month period for project and specialist task forces /Project teams set up. This is thus dependent on the European Commission notifying ESO's to start Phase 2 of Mandate 460 in June 2012.

The completion of the tasks and work items identified and associated to the above described work plans on the six areas of the Rationalised Structure will aim to fulfil the objectives of the rationalisation of the structure and presentation of the European Electronic Signature standardisation documents, i.e.:

- To allow business stakeholders to more easily implement and use products and services based on electronic signatures.
- 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.

Business driven guidance through the Guidance 19xx0 documents will be provided in the first stage of Phase 2 execution and should be completed within the first year.

The extension of the rationalised framework to include standards for electronic identification and authentication (as outlined in clause 5.3) will be studied to ensure that this work plan can be extended to include further standardisation for related standards for identification and authentication.

The rationalisation or the establishment of policy and security requirements as well as technical specifications, allowing an effective business driven approach, aiming to facilitate, clarify and ensuring eSignature implementations to the light of identified business requirements will be mostly completed after the second year of the execution of the Work Plan.

While the present work plan does not dig into the very last details, specific care will be taken during the execution of the second phase of the rationalisation exercise, not only in its definition stage but certainly in its execution stage 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.

Conformity Assessment Guidance and facilities for testing compliance and interoperability of eSignature implementations will similarly be completed after the second year of the execution of the Work Plan. In order to facilitate (cross-border) mutual recognition of eSignature based solutions, services and products, the execution of this part of the framework aims 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. This will similarly be completed after the second year of the execution of the Work Plan.

The provided timeframes include the necessary period for issuing European Norms whenever this is applicable.

In parallel and in a constant will of transparency and provision of a global and unique access point for presentation and download of standardisation documents, the website www.e-signatures-standards.eu will be regularly updated in accordance.

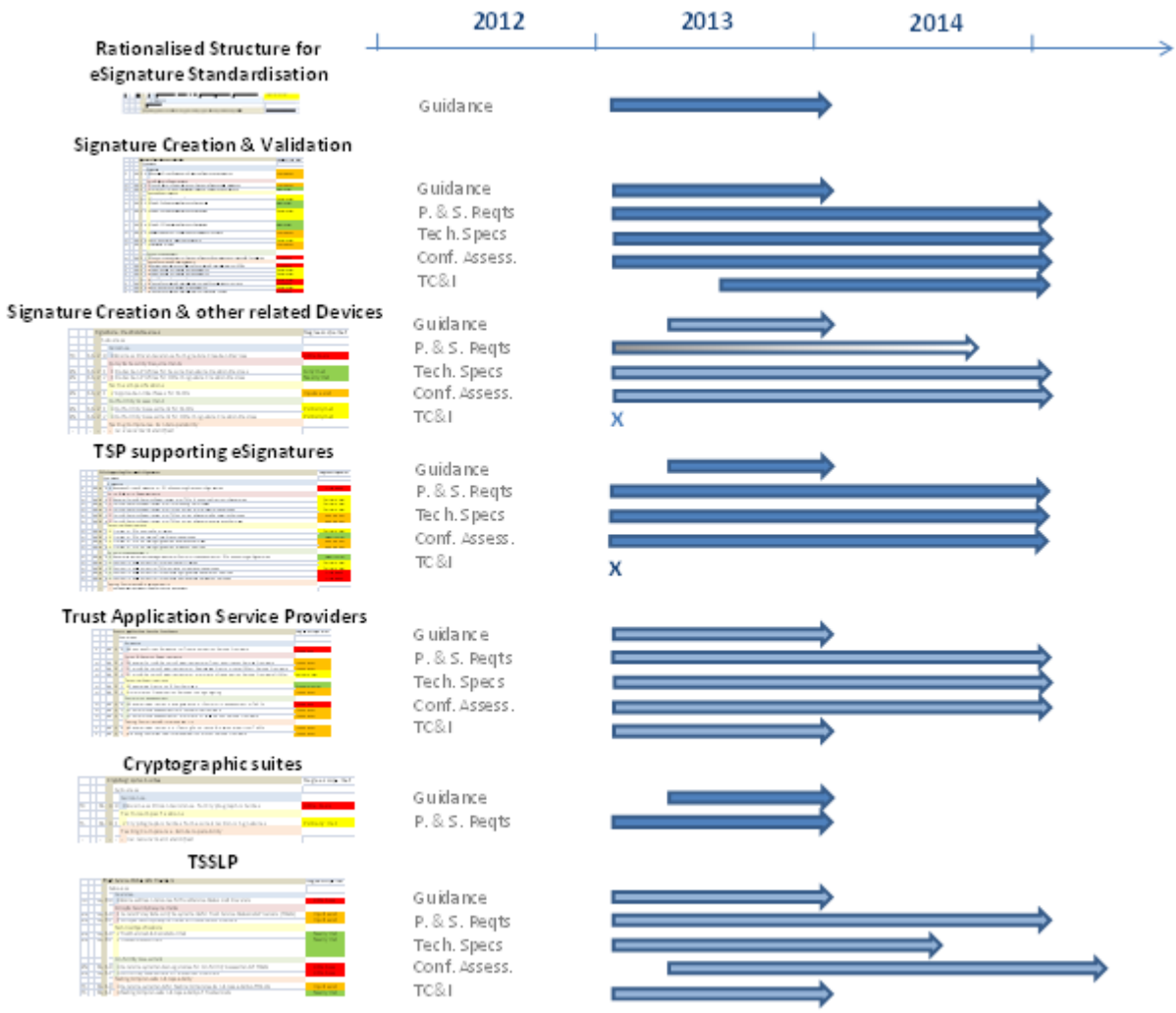


Figure 7: Overview of the consolidated work plan for the Rationalisation of the European eSignature Standardisation Framework

The next phase of the current rationalisation process will consist in ESO's (CEN, CENELEC and ETSI) to submit detailed proposal of work items and tasks to the European Commission once the present work plan and rationalised framework proposal will be under validation and approval. The drafting of such detailed proposals will be expected to be carried on during the second quarter of 2012 allowing time for the European Commission to comment and approve those proposals so that the effective work could start 2013.

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.

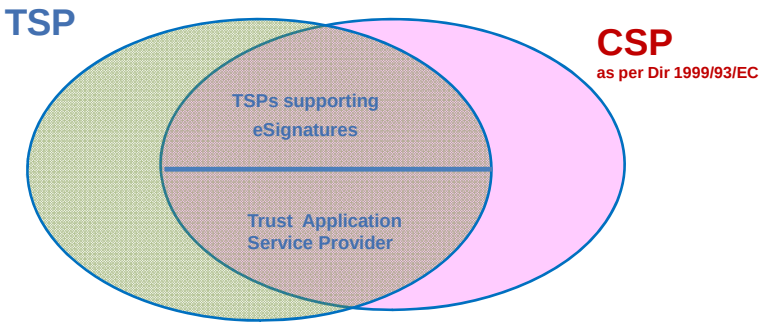


Figure A.1: Illustration of relationship between TSP and CSP

The term CSP as defined in Directive 1999/93/EC [i.1] 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 Output of Business Requirements Analysis to Electronic Signature Standards from Signature Creation/Validation Viewpoint

B.1 Introduction

A major new area identified in the Rationalised structure 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. It aims to assist businesses in the process of selection of standards but leaves businesses open to define their own requirements. It provides a language for businesses to describe its requirements and map them to standardisation solutions.

Within the present document businesses includes public administrations and not for profit organisations.

Note that this annex is to be the basis of future work to produce business guidance and is likely to be subject to significant change.

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

NOTE: Business requirements analysis is outside the scope of the guidance.

Based on this phased approach (requirements analysis, identification of business factors, selection of standards and technical rules for their implementation) illustrated in figure B.1, 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 19 101. 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 19 162.

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 validation 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 Open Document Format, 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 data to be signed 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 validation 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 CAB Forum 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 DIS 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 [i.14] 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 certificate 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 validation and the archival of the electronic signature and the validation data.

This may impact the selection of appropriate protection profiles and conformity assessment schemes against which the signature creation and validation 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 is to be used when a high risk is associated with erroneous authentication. (Qualified level or advanced level with qualified certificate)
(Comparable with LoA 4 as defined in ISO DIS 29115.)

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

NOTE 4: Requirements comparable with ISO DIS 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 data to be signed 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 data to be signed 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 validation 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 validation 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 validation 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:
Migration Strategy

Clause 5.2.4 proposes a consistent numbering scheme for electronic signature standardisation. The proposed strategy for migration to this numbering scheme is as follows:

a) ETSI and CEN secretariats are to agree on a number for the series (either 19 as suggested in the present document or some other agreed number.

b) New documents relating to electronic signatures which have not been allocated a number will be assigned number under the new scheme.

c) Where a document has already been allocated a number an updated version will be released which is an empty document referencing a new version under the new scheme.

Annex D: Inventory

Annex D is contained in archive sr_001604v010101p0.zip which accompanies the present document.

History

Document history		
V1.1.1	July 2012	Publication