ETSI TR 119 000 V1.2.1 (2016-04)

TECHNICAL REPORT

Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview

Reference

RTR/ESI-0019000v121

Keywords

e-commerce, electronic signature, security, trust services

ETSI

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

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

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

Important notice

Copyright Notification

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 (https://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 Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

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

Commission Decision 2003/511/EC [i.2], on generally recognized standards for electronic signature products, was adopted by the Commission following the results of the EESSI. This decision was aimed to foster the use of electronic signature by publishing "generally recognized standards" for electronic signature products in compliance with article 3(5) of the Directive. However, by referencing only two standards (respectively on security requirements for trustworthy systems managing certificates for electronic signatures and secure signature creation devices), it had a limited impact on the mapping of the European standardization on electronic signatures (which covers many more documents and topics, including ancillary services to electronic signature) and the legal provisions and requirements laid down in Directive 1999/93/EC [i.1].

Emerging cross-border use of electronic signatures 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 electronic signatures and the framework set by the eSignature Directive emphasized problems with the mutual recognition and cross-border interoperability of electronic signature.

Intending to address the legal, technical and standardization related causes of these problems, the Commission launched a study on the standardization aspects of electronic signature [i.7] which concluded that the 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 electronic signatures, 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 Standards (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 electronic signatures.

In line with Standardization Mandate 460 [i.9], consequently issued by the Commission to CEN, CENELEC and ETSI for updating the existing signature standardization 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 context of Mandate 460 was to establish a rationalized framework for signature standardization to overcome these issues within the context of the eSignature Directive, taking into account possible revisions to this Directive. In August 2014, the European Commission published Regulation 910/2014/EU of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [i.21]. That Regulation will effectively supersede Directive 1999/93/EC [i.1] on 1 July 2016. This brings within the scope of Regulation additional services for identification and authentication alongside an extended range of signature related trust services and defines additional forms of qualified certificates.

A work programme has been established and will be maintained to address any elements identified as missing in the framework for standardization of signatures. Unless specifically addressing specific types of legally defined electronic signatures (e.g. as in Directive 1999/93/EC [i.1] or in Regulation 910/2014/EU [i.21]), all documents of the framework intend to cover digital signatures supported by PKI and public key certificates [i.17], and aim to meet the general requirements of the international community to provide trust and confidence in electronic transactions, including, amongst other, applicable requirements from EU legislation [i.1] and [i.21]. Digital signatures are data appended to, or being a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery. They can enable, when appropriately supported by relevant trust services, implementation of electronic signatures and electronic seals as they are defined in the applicable European legislation [i.1] and [i.21].

1 Scope

The present document describes the general structure for ETSI/CEN digital signature standardization outlining existing and potential standards for such signatures, hereafter referred to as the framework for standardization of signatures. This framework identifies six areas of standardization with a list of existing and potential future standards in each area.

NOTE: Each title providing the name of a listed standard in the framework for standardization of signatures includes a hyperlink that leads to download facilities for such a standard, including all its versions, both as TS/TR and/or as EN when applicable.

2 References

2.1 Normative 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.

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

Not applicable.

2.2 Informative 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.

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

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] 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 https://ec.europa.eu/digital-agenda/en/news/study-standardisation-aspects-e-signatures-2007.

[i.8] "CROBIES: Study onCross-Border Interoperability of eSignatures", Siemens, SEALED and TimeLex, 2010.

NOTE: Available at https://ec.europa.eu/digital-agenda/en/news/crobies-study-cross-border-interoperability-esignatures-2010.

[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 Version 1.1", 11 April 2013.

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

[i.14] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[i.15] IETF RFC 3161 (August 2001): "Internet X.509 Public Key Infrastructure Time-Stamp Protocol".

[i.16] 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.17] Recommendation ITU-T X.509/ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.18] 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.19] 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.20] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[i.21] Regulation 910/2014/EU of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.22] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.23] Commission Decision 2013/662/EU of 14 October 2013 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.24] IETF RFC 5652 (2009): "Cryptographic Message Syntax (CMS)".

[i.25] Application Note: "APPNOTE.TXT - .ZIP File Format Specification", PKWARE® Inc., September 2012.

NOTE: Available at http://www.pkware.com/documents/APPNOTE/APPNOTE-6.3.3.TXT.

[i.26] Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[i.27] IETF RFC 4998: "Evidence Record Syntax (ERS)".

[i.28] IETF RFC 6283: "Extensible Markup Language Evidence Record Syntax (XMLERS)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 119 001 [i.22] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.22] apply.

4 General framework for standardization related to digital signatures

4.1 Introduction

4.1.1 Objectives

The objectives of the framework for standardization relating to digital signatures are:

a) To allow business stakeholders to more easily implement and use products and services based on digital signatures. A business driven approach, with guidance on the use of standards in business terms, underlies the framework. Business driven guidance are provided for maximizing successful implementation of signatures-based products, services and applications by guiding the stakeholders through the definition and parameterization of the different elements or components of signatures and/or signature-based services/applications and guiding them consequently through the selection of the appropriate standards and their implementation.

b) To facilitate mutual recognition and cross-border interoperability of signatures.

c) To simplify standards, reduce unnecessary options and avoid diverging interpretations of the standards.

d) To target a clear status of European Standard (EN) for standardization deliverables whenever this is applicable.

e) To facilitate a global presentation of the signature standardization landscape, the availability and access to the standards.

4.1.2 Approach

The central stone of the framework is the creation and validation of digital signatures. As business stakeholders even not familiar with signature underlying technology may already have deduced from Directive 1999/93/EC [i.1] and from Regulation 910/2014/EU [i.21], the creation and validation of signatures cannot be achieved in a fully open environment without relying on one or several third party services, tools or products. This namely covers digital certificate issuers to attest the identities of signers, 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 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 organizations.

Regulation (EU) No. 910/2014 [i.21] defines the terms electronic signature, advanced electronic signature, electronic seals and advanced electronic seal. These signatures and seals are usually created using digital signature technology. The framework for standardization of signatures aims at supporting the Regulation (EU) No 910/2014 [i.21] for creation and validation of advanced electronic signatures and seals when they are implemented as digital signatures in particular under the specific standardized CAdES, XAdES and PAdES signature formats (collectively denoted AdES signature formats), as well as the format for associated signature containers (ASiC).

For those target audiences, who are stakeholders willing to introduce and implement digital signatures in a business electronic process, the rationalized structure provides a viewpoint focusing on the creation/validation of digital signatures. This aims to guide them on how to implement digital signatures 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 also focuses on positioning creation/validation of digital signatures against the output of the provision of services supporting such creation/verification and potentially the preservation of such signatures. This viewpoint provides both guidance on defining and configuring the different signature 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 framework for standardization of signatures provides additional targeted guidance from the viewpoint of the trust service provider. This guidance focuses on the selection of standards relevant to particular trust services. Guidance is provided not only for trust service providers supporting digital signatures (e.g. trust service providers issuing qualified certificates) but also for those trust application providers offering value added services and applying digital signatures (e.g. registered electronic mail).

The framework focuses 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 digital signature based solutions, services and products, this framework also aims to provide a common basis for approval schemes through the definition of standard requirements for the assessment of such solutions, services and products against the 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.

4.2 Classification scheme for digital signature standards

4.2.1 Functional areas

The framework for standardization of signatures is organized around 6 (functional) areas and 5 types of documentation.

NOTE 1: Clause 4.2.5 addresses how this classification scheme can be expanded.

The 6 areas of the framework are the following:

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

    i) the policy and security requirements for signature creation, augmentation and validation applications;

    ii) the expression of rules and procedures to be followed at creation, augmentation, validation and for long term availability of signatures;

    iii) signature formats and packaging of signatures and signed documents; and

    iv) protection profiles, according to Common Criteria [i.16] for signature creation/augmentation/verification applications.

2) **Signature creation and other related devices:** This area focuses on standards related to secure signature creation devices as defined in Directive 1999/93/EC [i.1], on qualified signature creation devices as defined in Regulation 910/2014/EU [i.21], on signature creation devices used by trust service providers (TSPs) as well as other types of devices supporting signatures and related services such as authentication.

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

4) **Trust service providers supporting digital signatures and related services:** This includes TSPs issuing public keys certificates (both EU-qualified and non-qualified) to natural and legal persons, including web server certificates, time-stamping services providers, TSPs offering signature validation services, and TSPs offering remote signature creation services (also called signing servers). The current list covers those services supporting digital signature that exist to date; other trust services may be identified at a future date.

NOTE 2: The term "trust service provider supporting digital signature" is closely related to certification service provider (CSP) as defined in Directive 1999/93/EC [i.1]. See annex A for a discussion on the concept of TSP and CSP.

5) **Trust application service providers:** This covers TSPs offering value added services applying digital signatures and that rely on the generation/validation of 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 signatures are identified.

6) **Trust service status lists providers:** This area covers the standardization related to the provision of trust service status lists and the provision of trusted lists as defined, in the context of Directive 2006/123/EC [i.14] and Directive 1999/93/EC [i.1] by CD 2009/767/EC [i.18] as amended, and in the context of Regulation 910/2014/EU [i.21] by CID (EU) 2015/1505 [i.26].

An additional area, area 0 as depicted in figure 1, is gathering the present document as well as studies and other introductory deliverables related to the framework.

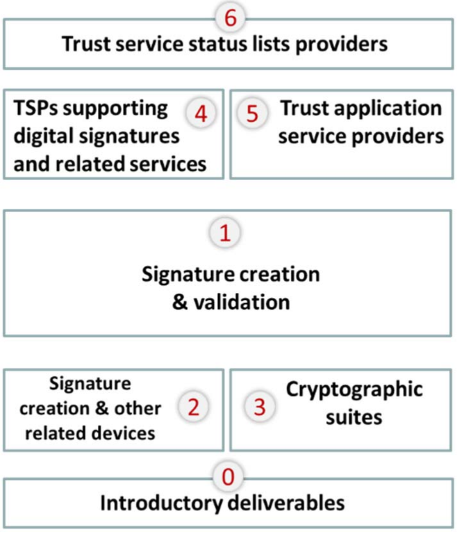

6
Trust service status lists providers
TSPs supporting digital signatures and related services
4
5
Trust application service providers
1
Signature creation & validation
Signature creation & other related devices
2
3
Cryptographic suites
0
Introductory deliverables

Figure 1: Overview of the structure of the framework for standardization of signatures

4.2.2 Document types

The documents required for standardization of each of the above functional areas have been organized around the following five types of documents:

0) **Guidance:** This type of document does not include any normative requirements but provides business driven guidance on addressing the signature (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.

1) **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.

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

3) **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).

4) **Testing conformance & 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.

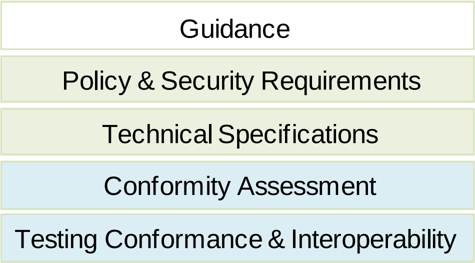

Guidance
Policy & Security Requirements
Technical Specifications
Conformity Assessment
Testing Conformance & Interoperability

Figure 2: Illustration of document types in the framework for standardization of signatures

4.2.3 Structure with sub-areas

This general area-based structure of the framework can be broken down into further sub-areas. This identifies the primary sub-areas within the six functional areas as described in clause 4.2.1. For each area, a common set of 5 types of document addresses 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, sub-areas have been identified focusing on the specific standardized CAdES, XAdES and PAdES signature formats, as well as the format for associated signature containers (ASiC) that bind together a number of signed data objects with signatures applied to them or time-stamp tokens computed on them. Digital signatures in mobile or distributed environments are also considered as part of this area.

In area 2, "signature creation and other related devices", documents are grouped in sub-areas with regards to the type of signature creation device, namely secure/qualified signature creation devices (SSCDs/QSCDs), devices for TSPs, for TSAs, for signing servers and authentication devices.

Area 4, TSPs supporting digital signatures and related services, has been divided in sub-areas focusing on the different types of such TSPs, namely trust service providers issuing certificates, time-stamping service providers, signature generation service providers and signature validation service providers.

Area 5, trust application service providers, contains three sub-areas, one dedicated to the provisioning of electronic registered delivery services, one to registered electronic mail (REM) services, and another one dedicated to data preservation service providers.

4.2.4 Numbering scheme

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

DD L19 xxx-z

Where:

DD indicates the deliverable type in the standardization 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 standardization 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 Standard (EN)
419 for CEN published Technical Report (TR), Technical Specification (TS) or European Standard (EN)

19 indicates the series of standardization documents related to signatures

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 and other related devices; 3-Cryptographic suites; 4-Trust service providers supporting digital signatures; 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 organization publishes the document.

4.2.5 Possible extension of classification scheme to incorporate identification and authentication related standards

Regulation 910/2014/EU [i.21] brings within the scope of regulation additional services for identification and authentication alongside signatures, namely to include electronic identification and authentication policy provisions.

A dedicated study and resulting Special Report document will consider, taking into account emerging technologies in identification and authentication, a possible extension to the classification and may suggest that these aspects can be incorporated in the structure of the framework 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 identification and authentication.

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

c) Further additional areas as needed for identification and authentication.

The classification of document types described in clause 4.2.2 is considered to be equally applicable to identification and authentication aspects.

4.2.6 Guidance documents addressing the framework functional areas

As a pre-requisite to the use of the respective guidance document, each stakeholder needs to describe and model, in a way as detailed as possible, the business domain, business process or business application in which the implementation of digital signature standards is looked for. This aims to ensure that all the details relating to crucial aspects of the business environment are captured and that the implementation of digital signatures does not miss any of them. This pre-requisite step also includes a risk assessment, as a way of getting the needed information from where policy and security requirements can be defined, so that once they are satisfied, stakeholders have a better assurance that the risks are identified and mitigated. The guidance documents, however do not aim at providing a complete guide on these topics but make readers aware of their relevance.

By elaborating the different sources of policy and security requirements into resulting control objectives and controls to be implemented in the system and by addressing and analysing the essential business scoping parameters in the context of the business process in which digital signature standards have to be implemented, the respective guidance documents will drive the stakeholders to the selection of standards and their options.

As illustrated in figure 3, a complete digital signatures solution may need to address requirements in several or most of the areas. However depending on the expectations of the stakeholders, the following documents can be used as starting points:

a) when a stakeholder is facing the need or wish to implement digital signatures in a business process, it can start with ETSI TR 119 100 on "Guidance on the use of standards for signature creation and validation";

b) when a stakeholder is facing the need or wish to use or design signature creation devices, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 200 on "Guidance on the use of standards for signature creation and other related devices" taking into account business requirements that come from other areas as shown in figure 3;

c) when a stakeholder is facing the need or wish to be advised on cryptographic suites, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 300 on "Guidance on the use of standards for cryptographic suites" taking into account business requirements that come from other areas as shown in figure 3;

d) when a stakeholder is facing the need or wish to provide TSP services either with the aim to issue certificates or to provide time-stamping services or to provide signature generation or validation services, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 400 on "Guidance on the use of standards for TSPs supporting digital signatures and related services" taking into account business requirements that come from other areas as shown in figure 3;

e) when a stakeholder is facing the need or wish to provide trust application service provider services either with the aim to provide electronic registered delivery services/registered electronic mail or to provide long term preservation services, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 500 on "Guidance on the use of standards for trust application service providers" taking into account business requirements that come from other areas as shown in figure 3;

f) when a stakeholder is facing the need or wish to publish approval status information on digital signature related trust services, it can consider the business scoping parameters and guided selection of standards as described in ETSI TR 119 600 on "Guidance on the use of standards for trust service status lists providers" taking into account business requirements that come from other areas as shown in figure 3.

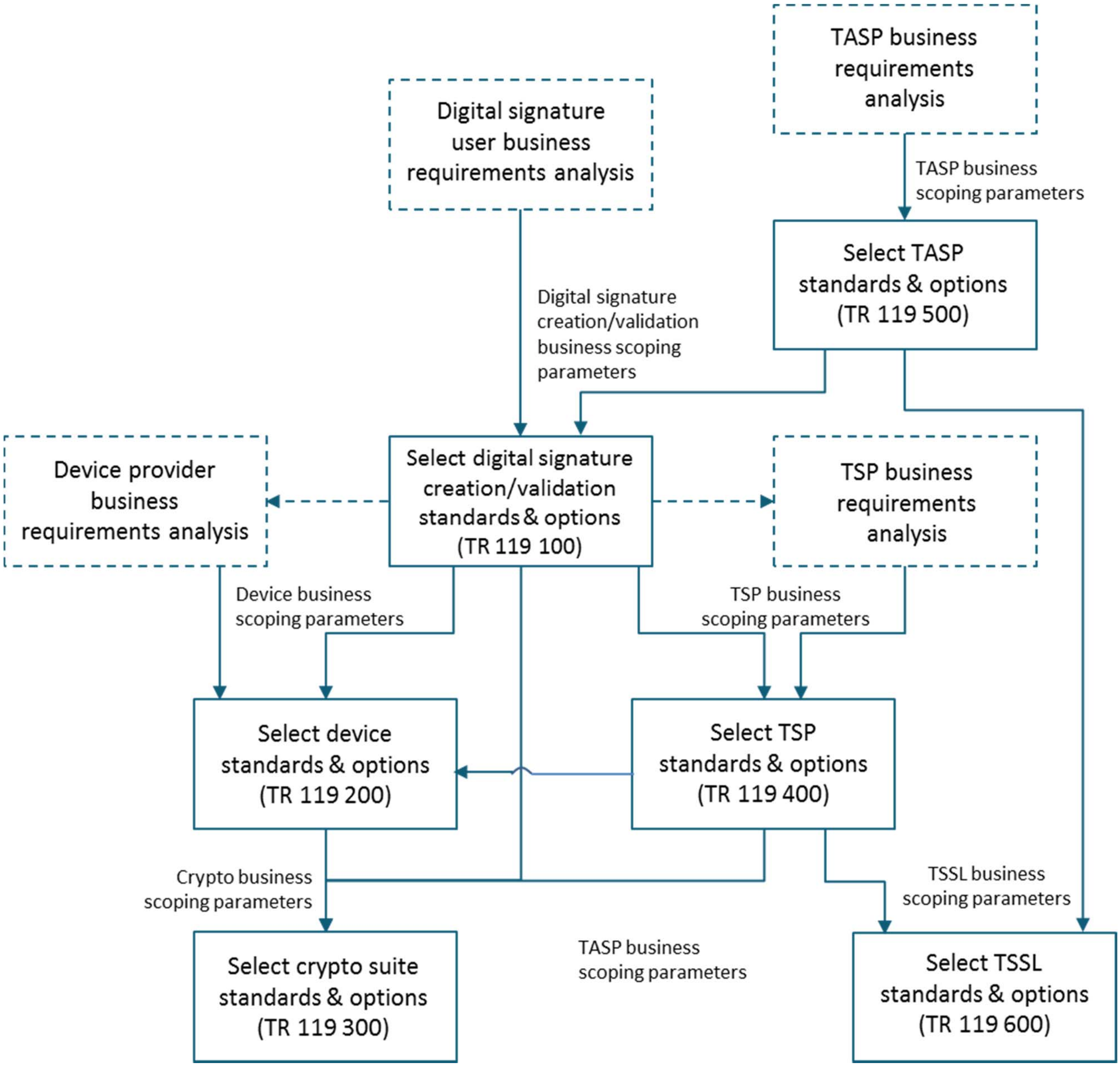

TASP business requirements analysis
TASP business scoping parameters
Digital signature user business requirements analysis
Select TASP standards & options (TR 119 500)
Digital signature creation/validation business scoping parameters
Device provider business requirements analysis
Select digital signature creation/validation standards & options (TR 119 100)
TSP business requirements analysis
Device business scoping parameters
TSP business scoping parameters
Select device standards & options (TR 119 200)
Select TSP standards & options (TR 119 400)
Crypto business scoping parameters
TSSL business scoping parameters
TASP business scoping parameters
Select crypto suite standards & options (TR 119 300)
Select TSSL standards & options (TR 119 600)

Figure 3: Dependencies of the business scoping parameters among the functional areas

4.3 The framework by area

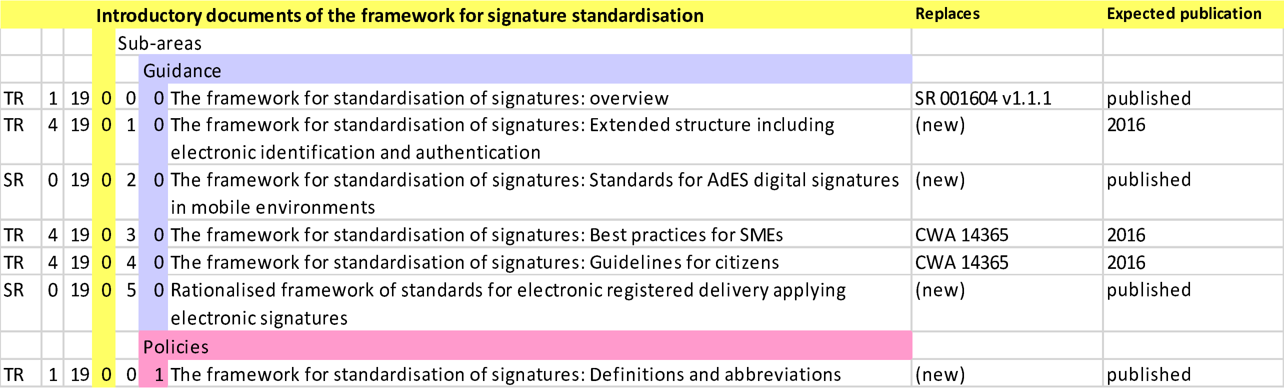
4.3.0 Foreword

The present clause identifies per area the different standards that are part of this area and provides for each of them a short description of its content and structure. Tables summarize the list of standards per area and indicate for each standard which standard or document it replaces when applicable and whether it is published or its planned publication date.

4.3.1 Introductory documents

The generic documents for digital signatures standardization are as summarized in table 1.

Table 1: Introductory documents of the framework for signature standardization



						Introductory documents of the framework for signature standardisation	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	0	0	0	The framework for standardisation of signatures: overview	SR 001604 v1.1.1	published
TR	4	19	0	1	0	The framework for standardisation of signatures: Extended structure including electronic identification and authentication	(new)	2016
SR	0	19	0	2	0	The framework for standardisation of signatures: Standards for AdES digital signatures in mobile environments	(new)	published
TR	4	19	0	3	0	The framework for standardisation of signatures: Best practices for SMEs	CWA 14365	2016
TR	4	19	0	4	0	The framework for standardisation of signatures: Guidelines for citizens	CWA 14365	2016
SR	0	19	0	5	0	Rationalised framework of standards for electronic registered delivery applying electronic signatures	(new)	published
						Policies		
TR	1	19	0	0	1	The framework for standardisation of signatures: Definitions and abbreviations	(new)	published

NOTE: Expected publication dates are provided for information and are subject to changes.

Guidance

ETSI TR 119 000 The framework for standardization of signatures: overview

The present document describes the general structure for digital signature standardization outlining existing and potential standards for such signatures. This framework identifies six areas of standardization with a list of existing and potential future standards in each area. It also provides the basis for business guidance provided in the other areas and references the guidance on the use of standards for signature creation and validation (ETSI TR 119 100) as the recommended starting point for the analysis of requirements in particular for those target audiences being stakeholders wishing to introduce and implement digital signatures in a business electronic process.

CEN TR 419 010 The framework for standardization of signatures: Extended structure including electronic identification and authentication

This document will propose an extension for the framework for standardization of signatures to cover identification, authentication and signatures.

ETSI SR 019 020 The framework for standardization of signatures: Standards for AdES digital signatures in mobile environments

This document will provide details on the framework of standards (including potential architectures and relevant scenarios) required for the creation and validation of AdES digital signatures in the mobile environment.

CEN TR 419 030 The framework for standardization of signatures: Best practices for SMEs

This document will provide best practices in the usage of digital signatures within the context of SMEs. It would answer to questions in relation with the use and benefits (ROI) of digital signatures to SMEs ecosystems.

CEN TR 419 040 The framework for standardization of signatures: Guidelines for citizens

This document will provide best practices in the usage of digital signatures within the context of citizens/consumers. It would answer to questions in relation with the use and benefits (ROI) of digital signatures to consumer's ecosystems.

ETSI SR 019 050 Rationalized framework of standards for electronic registered delivery applying electronic signatures

This document defines electronic delivery (e-delivery) services and investigate applicable requirements from those existing in the market (ETSI, CEN, private standards and pilots' outcome) proposing rationalized and well-organized requirements for electronic delivery applying digital signatures and its possible relation to registered electronic mail.

Policies

ETSI TR 119 001 The framework for standardization of signatures: Definitions and abbreviations

This document lists all definitions & abbreviations used in documents of the framework for standardization of signatures and serve as reference. Documents from the framework include definitions/abbreviations by reference to ETSI TR 119 001 [i.22] and/or by copying definitions from ETSI TR 119 001 [i.22].

4.3.2 Signature creation & validation

The standardization documents for signature creation and validation are summarized in table 2 with further details provided below.

Table 2: Standards for signature creation and validation

						Signature creation and validation	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	1	0	0	Guidance on the use of standards for signature creation and validation	(new) TR 102 047	published
						Policy & Security Requirements		
TS	1	19	1	0	1	Policy and security requirements for applications for signature creation and signature validation	(new)	published
EN	4	19	1	1	1	Protection profiles for signature creation and validation application - Part 1: Introduction to the European Norm - Part 2: Signature creation application - Core PP - Part 3: Signature creation application - Possible Extensions - Part 4: Signature verification application - Core PP - Part 5: Signature verification application - Possible Extensions	CWA/prEN 14170	All parts published in 2013-03 Parts 2 and 4 to be evaluated and certified in 2016-2017
						Technical Specifications		
EN	3	19	1	0	2	Procedures for creation and validation of AdES digital signatures - Part 1: Creation and validation - Part 2: Validation report	TS 102 853, CWA 14170, CWA 14171	Part 1: Apr. 2016 Part 2: undefined
EN	3	19	1	2	2	CAdES digital signatures - Part 1: Building blocks and CAdES baseline signatures - Part 2: Extended CAdES signatures	TS 101 733, TS 103 173, TS 102 734	Parts 1 & 2: Apr. 2016
EN	3	19	1	3	2	XAdES digital signatures - Part 1: Building blocks and XAdES baseline signatures - Part 2: Extended XAdES signatures	TS 101 903, TS 103 171, TS 102 904	Parts 1 & 2: Apr. 2016
EN	3	19	1	4	2	PAdES digital signatures - Part 1: Building blocks and PAdES baseline signatures - Part 2: Additional PAdES signatures profiles - Part 3: Visual representations of digital signatures	- TS 102 778-1 - TS 103 172 - TS 102 778-2/5 - TS 102 778-6	Parts 1 & 2: Apr. 2016 Part 3: delayed
TS	1	19	1	5	2	Architecture for AdES digital signatures in distributed environments	(new)	Undefined
EN	3	19	1	6	2	Associated Signature Containers (ASiC) - Part 1: Building blocks and ASiC baseline containers - Part 2: Additional ASiC containers	TS 102 918, TS 103 174	Parts 1 & 2: Apr. 2016
TS	1	19	1	7	2	Signature policies - Part 1: Building blocks and table of contents for human readable signature policy documents - Part 2: XML format for signature policies - Part 3: ASN.1 format for signature policies - Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists	- TR 102 041 / 045 - TR 102 038 - TR 102 272	- Part1: published - Other parts: undefined
						Conformity Assessment		
EN	4	19	1	0	3	Conformity assessment for signature creation & validation (applications & procedures)	(new) (CWA 14172-4 ?)	2016
						Testing Conformance & Interoperability		
TS	1	19	1	2	4	CAdES Testing conformance & interoperability	(new)	June 2016
TS	1	19	1	3	4	XAdES Testing conformance & interoperability	(new)	June 2016
TS	1	19	1	4	4	PAdES Testing conformance & interoperability	(new)	June 2016
TS	1	19	1	5	4	Testing conformance & interoperability of AdES in mobile environments	(new)	undefined
TS	1	19	1	6	4	ASiC Testing conformance & interoperability	(new)	June 2016

NOTE: Expected publication dates are provided for information and are subject to changes.

Guidance

ETSI TR 119 100 Guidance on the use of standards for signature creation and validation

This document provides guidance on the use of standards for the implementation of digital signature standards from the viewpoint of signature creation and validation. This will include guidance on selection between the different signature formats. It proposes a business driven guided process for implementing generation and validation of digital signatures in business' electronic processes. Starting from a business analysis and risk analysis of the business' electronic processes, stakeholders are guided for making the best choice among the wide offer of standards in order to ensure the best implementation of digital signatures within the addressed application / business electronic processes.

The process proposed by this guidance is defined in a way that ensures to stakeholders a proper and consistent treatment of all the business scoping parameters, explicitly taking into account:

a) parameters directly dependant on the specific application or business process;

b) parameters derived from the regulatory/legal framework where the business is conducted;

c) parameters inherent to the different types of signing entities; as well as

d) other aspects that do not fall within the above three listed categories but are important to be addressed when implementing digital signatures.

The purported audience of this document is rather wide and includes different readers' profiles, such as enterprise/business process architects or managers, business process standardization bodies, application architects, application developers, and signature policy issuers.

Policy and security requirements

ETSI TS 119 101 Policy and security requirements for applications for signature creation and signature validation

This document provides security requirements for applications creating, validating or augmenting digital signatures. This includes procedural aspects that are not directly machine processable, as well as aspects which can be defined in a machine processable way (see ETSI TS 119 172). This includes requirements for the secure operation of signature creation, augmentation and validation applications such as might be provided by an information security management system.

This document includes a standardized table of contents for a human readable document stating the signature application practices applied by signature creation applications, signature augmentation applications and/or signature validation applications in a considered business e-process environment.

Requirements for trust service providers providing signature creation or validation services are out of scope. General requirements for trust service providers are provided in ETSI EN 319 401. Requirements on trust service providers providing signature creation services are to be defined in ETSI TS 119 431, with CEN TS 419 241 defining requirements for a remote signature creation device. Requirements on trust service providers providing signature validation services are to be defined in ETSI TS 119 441.

NOTE: This takes into account the standards for information security management systems in ISO/IEC 27000 [i.10] family and templates for practice statements as in IETF RFC 3647 [i.11].

CEN EN 419 111 Protection Profiles for signature creation & validation application

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

Part 1: **Introduction to the European Norm:** This part is an introduction to the EN.

Part 2: **Signature creation application - Core PP:** This document is a protection profile for the signature creation application (SCA), specifying only the core security functions. 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/QCSD allows the signatory to generate an electronic signature.

Part 3: **Signature creation application - Possible Extensions:** This part specifies possible additional security functions that can be added to the core SCA PP.

Part 4: **Signature verification application - Core PP:** This document is a protection profile for the signature verification application (SVA), specifying only the core security functions. It defines security requirements for SVA conformity from the perspective of a security evaluation. The 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 validate an electronic signature.

Part 5: **Signature verification application - Possible Extensions:** This part specifies possible additional security functions that can be added to the core SVA PP.

Technical Specifications

ETSI EN 319 102 Procedures for creation and validation of AdES digital signatures

Part 1: **Creation and validation:** This document specifies procedures for:

- the creation of CAdES digital signatures (see ETSI EN 319 122-1), of XAdES digital signatures (see ETSI EN 319 132-1), or of PAdES digital signatures (see ETSI EN 319 142-1) respectively; and

- establishing whether a CAdES/XAdES/PAdES digital signature is technically valid;

within a given policy context, and whenever the CAdES/XAdES/PAdES digital signature is based on public key cryptography and supported by public key certificates.

This document introduces general principles, objects and functions relevant when creating or validating signatures based on signature creation and validation constraints and defines general classes of signatures that allow for verifiability over long periods.

Part 2: **Validation report:** This document will specify the contents and a format for reporting on the validation of AdES signatures as per what is specified in ETSI EN 319 102-1.

NOTE: A study is expected to be made for assessing the need of a separate part for supporting conformance testing of signature validation.

ETSI EN 319 122 CAdES digital signatures

This multi-part document contains all the specifications related to CAdES digital signatures built on top of CMS signatures [i.24] by incorporation of signed and unsigned attributes. It includes specifications for baseline and for extended CAdES digital signatures:

Part 1: **Building blocks and CAdES baseline signatures:** This document specifies the ASN.1 definitions for the signed and unsigned attributes that are added to CMS signatures to become CAdES signatures and their usage when incorporating them in CAdES signatures building from CMS signatures. This document specifies formats for CAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications. CAdES baseline signatures are applicable to a wide range of communities when there is a clear need for interoperability of digital signatures on electronic documents. Four levels of CAdES baseline signatures are defined addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Each level requires the presence of certain CAdES attributes, suitably profiled for reducing the optionality as much as possible.

Part 2: **Extended CAdES signatures:** This document specifies a number of CAdES signature levels addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Those CAdES extended signatures offer a higher degree of optionality than the CAdES baseline signatures specified in part 1 of ETSI EN 319 122.

NOTE: The baseline profile 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.14].

ETSI EN 319 132 XAdES digital signatures

This multi-part document contains all the specifications related to AdES digital signatures built on top of XML signatures [i.12] by incorporation of signed and unsigned properties. It includes specifications for baseline signatures and for extended XAdES digital signatures:

Part 1: **Building blocks and XAdES baseline signatures:** This document specifies the XML Schema definitions for the signed and unsigned qualifying properties that are incorporated into XML signatures to become XAdES signatures and the mechanisms to incorporate them into XAdES signatures. This document specifies formats for XAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications. XAdES baseline signatures are applicable to a wide range of communities when there is a clear need for interoperability of digital signatures on electronic documents. Four levels of XAdES baseline signatures are defined addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Each level requires the presence of certain XAdES qualifying properties, suitably profiled for reducing the optionality as much as possible.

Part 2: **Extended XAdES signatures:** This document specifies a number of XAdES signature levels addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Those CAdES extended signatures offer a higher degree of optionality than the XAdES baseline signatures specified in part 1 of ETSI EN 319 132.

NOTE: The baseline profile 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.14].

ETSI EN 319 142 PAdES digital signatures

This multi-part document contains all the specifications related to digital signatures embedded within PDF documents. It includes PAdES baseline signature specifications and additional profiles, and in particular:

Part 1: **Building blocks and PAdES baseline signatures:** This document specifies PAdES digital signatures building on PDF signatures specified in ISO 32000-1 [i.13] with an alternative signature encoding to support digital signature formats equivalent to the signature format CAdES as specified in ETSI EN 319 122-1, by incorporation of signed and unsigned attributes, which fulfil certain common requirements (such as the long term validity of digital signatures) in a number of use cases.

This document specifies formats for PAdES baseline signatures, which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications. PAdES baseline signatures are applicable to a wide range of communities when there is a clear need for interoperability of digital signatures used in electronic documents.

Four levels of PAdES baseline signatures are defined addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. Each level requires the presence of certain PAdES attributes, suitably profiled for reducing the optionality as much as possible.

Part 2: **Additional PAdES signatures profiles:** This document defines multiple profiles for PAdES digital signatures which are digital signatures embedded within a PDF file.

This document contains a profile for the use of PDF signatures, as described in ISO 32000-1 [i.13] and based on CMS digital signatures [i.24], that enables greater interoperability for PDF signatures by providing additional restrictions beyond those of ISO 32000-1 [i.13]. This first profile is not related to part 1 of ETSI EN 319 142.

It also contains a second set of profiles that extend the scope of the profile in ETSI EN 319 142 part 1, while keeping some features that enhance interoperability of PAdES signatures. Those profiles define three levels of PAdES extended signatures addressing incremental requirements to maintain the validity of the signatures over the long term, in a way that a certain level always addresses all the requirements addressed at levels that are below it. These PAdES extended signatures offer a higher degree of optionality than the PAdES baseline signatures specified in part 1 of ETSI EN 319 142.

A third profile is defined for usage of an arbitrary XML document signed with XAdES signatures that is embedded within a PDF file.

Part 3: **Visual representations of digital signatures:** This document will specify requirements and recommendations for the visual representations of digital signatures in PDFs. This covers:

a) Signature appearance: The visual representation of the human act of signing placed within a PDF document at signing time and linked to a digital signature.

b) Signature verification representation: The visual representation of the validation of a digital signature.

The aim of the document is to provide requirements and recommendations for signature appearances and the visual representation of digital signatures. This is particularly aimed to help the untrained human observer to understand the signature and to extend the consistency between the signature appearance and the visual representations of the AdES verification in order to help human comparison.

It includes further explanation of two different visual representations of digital signatures related to PDF but does not cover printable forms of signature values (e.g. using barcodes) which may be verifiable from the printed document.

NOTE: The baseline profile 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.14].

ETSI TS 119 152 Architecture for AdES digital signatures in distributed environments

This document will identify the architectural components, protocol requirements and sequence of interactions required for scenarios based on those in ETSI SR 019 020.

ETSI EN 319 162 Associated Signature Containers (ASiC)

This multi-part document contains all the specifications related to the so-called Associated Signature Containers. Such containers bind together into one single digital container based on ZIP [i.25] either detached digital signatures or time assertions, with a number of file objects (e.g. documents, XML structured data, spreadsheet, multimedia content) to which they apply. It includes specifications for ASiC baseline containers and for additional ASiC containers, and in particular:

Part 1: **Building blocks and ASiC baseline containers:** This document specifies the format for a single digital container based on ZIP [i.25] binding together a number of signed objects (e.g. documents, XML structured data, spreadsheet, multimedia content) with either AdES or time assertions. ASiC supports the following signature and time assertion formats: CAdES object incorporating CAdES signatures (see ETSI EN 319 122), XAdES signatures (see ETSI EN 319 132), IETF RFC 3161 [i.15] and updated by IETF RFC 5816 [i.20] time-stamp tokens, and IETF RFC 4998 [i.27] or IETF RFC 6283 [i.28] evidence records.

The building blocks defined in this document support additional features not supported by the aforementioned formats, such as time-stamping and CAdES signing of multiple content and XAdES parallel signatures, that can be used in other contexts.

This document defines baseline containers which provide the basic features necessary for a wide range of business and governmental use cases for electronic procedures and communications. Baseline containers are applicable to a wide range of communities when there is a clear need for interoperability.

Four levels of ASiC baseline containers are defined addressing incremental requirements to maintain the availability and integrity of the containers over the long term, suitably profiled for reducing the optionality as much as possible, in a way that a certain level always addresses all the requirements already addressed at levels that are below it.

Part 2: **Additional ASiC containers:** Specific communities or use cases may have additional requirements that are not addressed by the baseline containers defined in part 1 that can be built using the building blocks defined there or additional ones. The document references such specific additional use of ASiC and aims to be used for containers that collect together electronic documents including those supported by OCF, ODF and UCF describing how these container formats can be used to associate digital signatures with any data objects in the container.

NOTE: The baseline containers take 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.14].

ETSI TS 119 172 Signature policies

This document addresses signature policies usable in the management of digital signatures within extended business models. This is a multi-part document whose internal structure is shown below:

Part 1: **Building blocks and table of contents for human readable signature policy documents:** This document defines the building blocks of signature policy and specifies a table of contents for human readable signature policy documents.

Part 2: **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 validating applications.

Part 3: **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 validating applications.

Part 4: **Signature validation policy for European qualified electronic signatures/seals using trusted lists:** This document will specify a signature validation policy using trusted lists that may be used for European qualified electronic signatures/seals and advanced electronic signatures/seals supported by qualified certificates in Europe.

Conformity Assessment

CEN EN 419 103 Conformity assessment for signature creation and validation (applications & procedures)

This document will introduce the following 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 digital signature creation and validation against protection profiles.

c) Assessment of conformity to AdES 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 Conformance & Interoperability

ETSI TS 119 124 CAdES testing conformance & interoperability

This document will first define test suites for supporting the organization of interoperability testing events where different CAdES related applications can check their actual interoperability. Additionally, it will define a complete set of test assertions for testing technical conformance of CAdES signatures against the relevant CAdES technical specifications. This document will help implementers and will likely accelerate the development of CAdES signature creation and validation applications. The test results can also be used in conformity assessment for signature creation and validation applications (ETSI EN 319 103) with policies requiring conformity to CAdES formats and procedures.

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

ETSI TS 119 134 XAdES testing conformance & interoperability

This document will first define test suites for supporting the organization of interoperability testing events where different XAdES related applications can check their actual interoperability. Additionally, it will define a complete set of test assertions for testing technical conformance of XAdES signatures against the relevant XAdES technical specifications. This document will help implementers and will likely accelerate the development of XAdES signature creation and validation applications. The test results can also be used in conformity assessment for signature creation and validation applications (ETSI EN 319 103) with policies requiring conformity to XAdES formats and procedures.

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

ETSI TS 119 144 PAdES testing conformance & interoperability

This document will first define test suites for supporting the organization of interoperability testing events where different PAdES related applications can check their actual interoperability. Additionally, it will define a complete set of test assertions for testing technical conformance of PAdES signatures against the relevant PAdES technical specifications. This document will help implementers and will likely accelerate the development of PAdES signature creation and validation applications. The test results can also be used in conformity assessment for signature creation and validation applications (ETSI EN 319 103) with policies requiring conformity to PAdES formats and procedures.

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

ETSI TS 119 154 Testing conformance & interoperability of AdES in mobile environments

This document will provide technical specifications for helping implementers and accelerating the development of creation and validation applications for AdES in mobile environments.

ETSI TS 119 164 ASiC testing conformance & interoperability

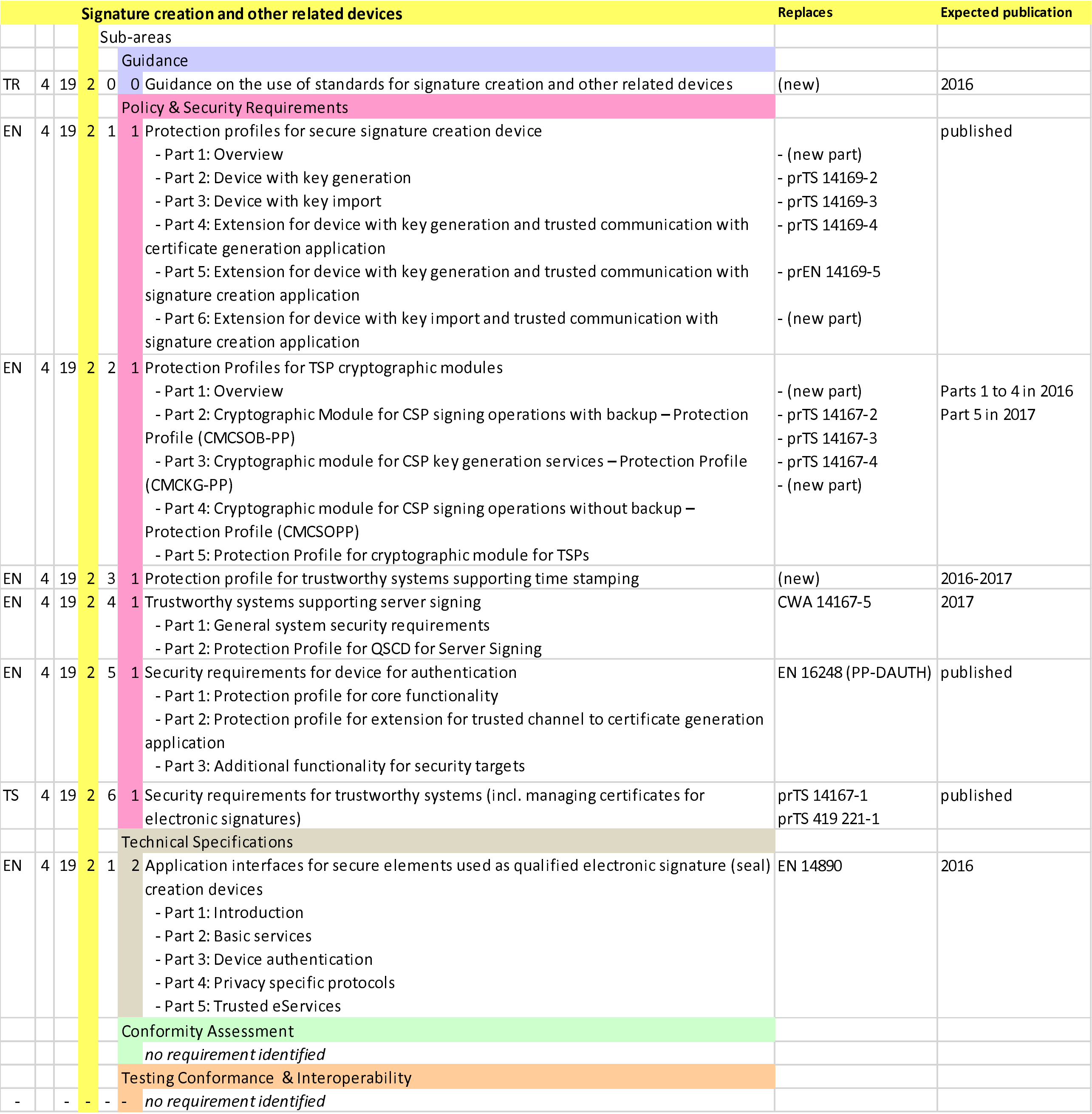
This document will first define test suites for supporting the organization of interoperability testing events where different ASiC container creation and validation applications can check their actual interoperability. Additionally, it will define a complete set of test assertions for testing technical conformance of ASiC against the relevant technical specifications. This document will help implementers and will likely accelerate the development of ASiC creation and validation applications. The test results can also be used in conformity assessment for signature creation and validation applications (ETSI EN 319 103) with policies requiring conformity to ASiC formats and procedures.

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

4.3.3 Signature creation and other related devices

The standardization documents for signature creation and other related devices are summarized in table 3 with further details provided below.

Table 3: Standards for signature creation and other related devices



			Signature creation and other related devices				**Replaces**	**Expected publication**
				Sub-areas				
					Guidance			
TR	4	19	2	0	0	Guidance on the use of standards for signature creation and other related devices	(new)	2016
					Policy & Security Requirements			
EN	4	19	2	1	1	Protection profiles for secure signature creation device		published
						- Part 1: Overview	- (new part)	
						- Part 2: Device with key generation	- prTS 14169-2	
						- Part 3: Device with key import	- prTS 14169-3	
						- Part 4: Extension for device with key generation and trusted communication with certificate generation application	- prTS 14169-4	
						- Part 5: Extension for device with key generation and trusted communication with signature creation application	- prEN 14169-5	
						- Part 6: Extension for device with key import and trusted communication with signature creation application	- (new part)	
EN	4	19	2	2	1	Protection Profiles for TSP cryptographic modules		
						- Part 1: Overview	- (new part)	Parts 1 to 4 in 2016
						- Part 2: Cryptographic Module for CSP signing operations with backup – Protection Profile (CMCSOB-PP)	- prTS 14167-2	Part 5 in 2017
						- Part 3: Cryptographic module for CSP key generation services – Protection Profile (CMCKG-PP)	- prTS 14167-3	
						- Part 4: Cryptographic module for CSP signing operations without backup – Protection Profile (CMCSOPP)	- prTS 14167-4	
						- Part 5: Protection Profile for cryptographic module for TSPs	- (new part)	
EN	4	19	2	3	1	Protection profile for trustworthy systems supporting time stamping	(new)	2016-2017
EN	4	19	2	4	1	Trustworthy systems supporting server signing	CWA 14167-5	2017
						- Part 1: General system security requirements		
						- Part 2: Protection Profile for QSCD for Server Signing		
EN	4	19	2	5	1	Security requirements for device for authentication	EN 16248 (PP-DAUTH)	published
						- Part 1: Protection profile for core functionality		
						- Part 2: Protection profile for extension for trusted channel to certificate generation application		
						- Part 3: Additional functionality for security targets		
TS	4	19	2	6	1	Security requirements for trustworthy systems (incl. managing certificates for electronic signatures)	prTS 14167-1 prTS 419 221-1	published
					Technical Specifications			
EN	4	19	2	1	2	Application interfaces for secure elements used as qualified electronic signature (seal) creation devices	EN 14890	2016
						- Part 1: Introduction		
						- Part 2: Basic services		
						- Part 3: Device authentication		
						- Part 4: Privacy specific protocols		
						- Part 5: Trusted eServices		
					Conformity Assessment			
						no requirement identified		
					Testing Conformance & Interoperability			
-		-	-	-	-	*no requirement identified*		

NOTE: Expected publication dates are provided for information and are subject to changes.

Guidance

CEN TR 419 200 Guidance on the use of standards for signature creation and other related devices

This document provides guidance for the use and selection of standards for signature creation and other related 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 security requirements of the signing environment in ETSI TS 119 101.

CEN EN 419 211 Protection profiles for secure signature creation device

This document specifies the security requirements for a SSCD that is the target of evaluation. It follows the rules and formats of the Common Criteria v3 [i.16].

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

Part 1: **Overview:** An introduction to the SSCD protection profiles.

Part 2: **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 can be extended through extensions specified in other parts.

Part 3: **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.

Part 4: **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 can be extended through extensions specified in other parts.

Part 5: **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.

Part 6: **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.

A companion document for CEN EN 419 211 will be produced to match the terminology between Directive 1999/93/EC [i.1] and Regulation 910/2014/EU [i.21], since CEN EN 419 211 has been delivered before the publication of that Regulation.

CEN EN 419 221 Protection profiles for TSP cryptographic modules

This multi-part document specifies protection profiles for cryptographic devices used by trust service providers. It covers the following topics:

Part 1: **Overview:** This part provides an overview of the protection profiles specified in other parts of CEN EN 419 221.

Part 2: **Cryptographic module for CSP signing operations with backup - Protection Profile (CMCSOB-PP):** This part specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93 [i.1]) for signing operations, with key backup, at a high level of security. Target applications include root certification authorities (certification authorities who issue certificates to other CAs and who are at the top of a CA hierarchy) and other certification service providers where there is a high risk of direct physical attacks against the module.

Part 3: **Cryptographic module for CSP key generation services - Protection Profile (CMCKG-PP):** This part specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93 [i.1]) for generating signing keys for use by other parties, at a high level of security. Target applications include root certification authorities and other certification service providers where there is a high risk of direct physical attacks against the module.

Part 4: **Cryptographic module for CSP signing operations without backup - Protection Profile (CMCSOPP):** This part specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93 [i.1]) for signing operations, without key backup, at a high level of security. Target applications include root certification authorities (certification authorities which issue certificates to other CAs and is at the top of a CA hierarchy) and other certification service providers where there is a high risk of direct physical attacks against the module.

Part 5: **Cryptographic module for trust services:** This part specifies a protection profile for cryptographic modules used by trust service providers for providing trust services (e.g. signing operations and authentication services) at a moderate level of security. This protection profile includes support for protected backup of keys. The target of this part is:

a) provision of cryptographic support for TSP signing operations including applications such as certification authorities who issue qualified and non-qualified certificates to end users, level 1 signing services as identified in CEN EN 419 241, data "sealing" by or on behalf of a legal entity, time-stamping services and validation services; and

b) provision of both symmetric and asymmetric cryptographic support for TSP authentication services, for example for authenticating users of signing services as specified in CEN EN 419 241.

This profile assumes that the cryptographic module is in a physically secured environment and that there is a low risk of untrusted personnel having direct physical access to the device.

While parts 2, 3 and 4 are Directive 1999/93/EC [i.1] oriented, but eIDAS Regulation [i.21] compliant, part 5 is focused on cryptographic modules used by TSP to provide signing operations (remote or server signing) and authentication services.

CEN EN 419 231 Protection profile for trustworthy systems supporting time stamping

This document defines protection profiles for a time-stamping trustworthy system that consists of at least a time-stamping unit (namely a set of hardware including an internal clock and software creating time-stamp tokens) and of administration and auditing facilities used to provide time-stamping services.

CEN EN 419 241 Trustworthy systems supporting server signing

This document is a multi-part document including general security requirements and protection profiles for trustworthy systems supporting server signing:

Part 1: **General system security requirements**.

Part 2: **Protection Profile for QSCD for Server Signing**.

The document is intended for use by developers and evaluators of a server signing application and of its components.

CEN EN 419 251 Security requirements for device for authentication

This multi-part document defines protection profiles 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:

Part 1: **Protection profile for core functionality**.

Part 2: **Protection profile for extension for trusted channel to certificate generation application**.

Part 3: **Additional functionality for security targets**: that can be added to part 1 or part 2 in order to define a new PP with enhanced features.

CEN TS 419 261 Security requirements for trustworthy systems (incl. managing certificates for electronic signatures)

This document establishes security requirements for trustworthy systems and technical components that can be used by a TSP in order to issue EU qualified and non-qualified certificates.

Technical specifications

CEN EN 419 212 Application interfaces for secure elements used as qualified electronic signature (seal-) creation devices

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

This multi-part document covers the following topics:

Part 1: **Introduction:** This part introduces the different parts of the series and gives the main notions and common definitions.

Part 2: **Basic services:** This part describes the specifications for signature (and seal) generation, including user verification, password-based authentication protocols, establishment of a secure channel and key generation. A specific annex deals with seal, and another one with remote signature.

Part 3: **Device authentication:** This part describes device authentication protocols, including data structures, Card-Verifiable (CV) certificates and key management.

Part 4: **Privacy specific protocols:** This document describes privacy specific protocols.

Part 5: **Trusted eServices:** This document describes additional trusted e-services in the context of signature including Client/Server authentication, role authentication, symmetric key transmission between a remote server and a SE, signature cryptographic verification.

Conformity Assessment

No requirements identified so far for such documents.

Technical Conformance & Interoperability Testing

No requirements identified so far for such documents.

4.3.4 Cryptographic suites

The standardization documents for cryptographic suites are summarized in table 4 with further details provided below.

Table 4: Standards for cryptographic suites

						Cryptographic suites	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	3	0	0	Guidance on the use of standards for cryptographic suites	(new)	published
						Technical Specifications		
TS	1	19	3	1	2	Cryptographic suites	TS 102 176-1	published
						Testing Conformance & Interoperability		
-		-	-	-	-	*no requirement identified*		

NOTE: Expected publication dates are provided for information and are subject to changes.

Guidance

ETSI TR 119 300 Guidance on the use of standards for cryptographic suites

This document provides business driven guidance on the use of standards for cryptographic suites, and in particular for digital signature creation algorithms.

It explains the concept of security parameters that helps to choose a proper cryptographic suite for digital signature creation. It also gives an overview how to analyse the business needs and how to select a system that satisfies these needs.

The purported audience of this document is mainly the application designers and implementers. It provides recommendations to trust service providers and manufacturers of security devices.

Technical Specifications

ETSI TS 119 312 Cryptographic Suites

This document specifies cryptographic suites used for digital signature creation and verification algorithms.

It provides guidance on selection of cryptographic suites corresponding to the appropriate level of security, which fulfils the security needs identified during the system design. It identifies a range of alternative cryptographic suites. There is no normative requirement on selection among the alternatives but for all alternatives, normative requirements apply to ensure security and interoperability.

This document also provides guidance on the hash functions, signature schemes and signature suites to be used with the data structures used in the context of digital signatures. For each data structure, the set of algorithms to be used is specified.

Conformity Assessment

No requirements identified so far for such documents.

Technical Conformance & Interoperability Testing

No requirements identified so far for such documents.

4.3.5 TSPs supporting digital signatures and related services

The standardization documents for TSPs supporting digital signatures and related services are summarized in table 5 with further details provided below.

Table 5: Standards for TSPs supporting digital signatures and related services

						TSPs supporting digital signatures and related services	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	4	0	0	Guidance on the use of standards for TSPs supporting digital signatures and related services	(new)	published
						Policy & Security Requirements		
EN	3	19	4	0	1	General policy requirements for trust service providers	Replacing generic parts of TS 101 456, TS 102 042, (TR 102 040), TS	published
EN	3	19	4	1	1	Policy and security requirements for trust service providers issuing certificates - Part 1: General requirements - Part 2: Requirements for trust service providers issuing EU qualified certificates - Part 3: *To be withdrawn* - Part 4: Requirements for trust service providers issuing code signing certificates	- TS 102 042 (EV & BR), EN 319 411-3 - TS 101 456 (& TR 102 458), EN 319 411-3 - historical - (new)	- published - published - withdrawn - undefined
EN	3	19	4	2	1	Policy & security requirements for trust service providers issuing time-stamps	TS 102 023	published
EN	3	19	4	3	1	Policy and security requirements for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	1	Policy and security requirements for trust service providers providing AdES digital signature validation services	(new)	Undefined
						Technical Specifications		
EN	3	19	4	1	2	Certificate profiles - Part 1: Overview and common data structures - Part 2: Certificate profile for certificates issued to natural persons - Part 3: Certificate profile for certificates issued to legal persons - Part 4: Certifcate profile for web site certificates - Part 5: QCStatements	- (new part) - TS 102 280 & TS 101 862 - (new part) - (new part) - TS 101 862	all parts published
EN	3	19	4	2	2	Time-stamping protocol and time-stamp token profiles	TS 101 861	published
EN	3	19	4	3	2	Protocol profiles for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	2	Protocol profiles for trust service providers providing AdES digital signature validation services	(new)	Undefined
						Conformity Assessment		
EN	3	19	4	0	3	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing trust service providers	CWA 14172 (2&8), TS 119 403	published
						Testing Conformance & Interoperability		
-	-	-	-	-	-	*no requirement identified for such a document*		

NOTE: Expected publication dates are provided for information and are subject to changes.

Guidance

ETSI TR 119 400 Guidance on the use of standards for TSPs supporting digital signatures

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

NOTE: When the need arises for identifying and producing specific business driven guidance for specific types of TSPs supporting digital signatures, the framework model allows the creation of ETSI TR 119 410, ETSI TR 119 420, ETSI TR 119 430, etc. documents for such purpose.

Policy & Security Requirements

ETSI EN 319 401 General policy requirements for trust service providers

This document specifies policy requirements for TSPs that are independent of the type of TSP whether certificate issuer (qualified or otherwise), timestamp issuer, signature verifier, e-delivery provider or other form of trust service provider. It defines policy requirements on the operation and management practices of TSPs.

ETSI EN 319 411 Policy and security requirements for trust service providers issuing certificates

This multi-part document specifies policy and security requirements for TSPs issuing certificates. It references ETSI EN 319 401 for generic requirements.

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

Part 1: **General requirements:** This part specifies generally applicable policy and security requirements for TSPs issuing public key certificates, including trusted web site certificates. The policy and security requirements are defined in terms of requirements for the issuance, maintenance and life-cycle management of certificates. These policy and security requirements support a number of reference certificate policies (LCP, NCP, NCP+, EVCP, OVCP, DVCP).

Part 2: **Requirements for trust service providers issuing EU qualified certificates:** This part specifies policy and security requirements for TSPs issuing EU qualified certificates as defined in Regulation 910/2014/EU [i.21]. These policy and security requirements support reference certificate policies (QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd, QCP-w) for the issuance, maintenance and life-cycle management of EU qualified certificates issued to natural persons (including natural persons associated with a legal person), to legal persons and to web sites.

Both documents provide informative annexes with a check list of the policy requirements that can be used by the TSP to prepare an assessment of its practices against the document and/or by the assessor when conducting the assessment for confirming that a TSP meets those requirements.

Part 3: Previously published ETSI EN 319 411-3 standard will be withdrawn. Content of that document has been split into the more recent versions of the first two parts.

Part 4: Requirements for trust service providers issuing code signing certificates: This document will specify requirements for TSPs issuing code signing certificates to ensure that one of the most widespread uses of electronic seals to protect digital assets can be aligned with international TSP practices such as those defined by the CA Browser forum.

ETSI EN 319 421 Policy and security requirements for trust service providers issuing time-stamps

This document specifies policy and security requirements relating to the operation and management practices of TSPs issuing time-stamps and references ETSI EN 319 401 for generic requirements. Those policy requirements are applicable to TSPs issuing time-stamps. Such time-stamps can be used in support of digital signatures or for any application requiring to prove that a data existed before a particular time. The document can be used by independent bodies as the basis for confirming that a TSP can be trusted for issuing time-stamps.

Similarly to ETSI EN 319 411, an informative annex provides check lists that can be used by the TSP to prepare an assessment of its practices against the document and/or by the assessor when conducting the assessment for confirming that a TSP meets those requirements.

ETSI EN 319 431 Policy and security requirements for trust service providers providing AdES digital signature generation services

This document will specify policy requirements for TSPs providing signature generation services. It will reference ETSI EN 319 401 for generic requirements.

Similarly to ETSI EN 319 411, informative annexes will provide check lists for conformity assessment.

ETSI EN 319 441 Policy and security requirements for trust service providers providing AdES digital signature validation services

This document will specify policy requirements for TSPs providing Signature Validation Services. It will reference ETSI EN 319 401 for generic requirements.

Similarly to ETSI EN 319 411, informative annexes will provide check lists for conformity assessment.

Technical Specifications

ETSI EN 319 412 Certificate profiles

This document provides specifications for specific profiles for use by TSPs issuing certificates including EU qualified and other forms of certificates. It provides certificate profiles and a set of specific statement extensions which aim to facilitate interoperability of (EU qualified) certificates issued to natural person, legal person or to organization as website certificate, for the purposes of (EU qualified) electronic signatures, (EU qualified) electronic seals, peer entity authentication, data authentication, as well as data confidentiality.

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

Part 1: **Overview and common data structures**.

Part 2: **Certificate profile for certificates issued to natural persons**.

Part 3: **Certificate profile for certificates issued to legal persons**.

Part 4: **Certificate profile for web site certificates**.

Part 5: **QCStatements**.

ETSI EN 319 422 Time-stamping protocol and time-stamp token profiles

This document defines a profile for the time-stamping protocol and the time-stamp token defined in IETF RFC 3161 [i.15] including optional ESSCertIDv2 update in IETF RFC 5816 [i.20]. It defines what a time-stamping client supports and what a time-stamping server supports. Time-stamp validation is out of scope and is defined in ETSI EN 319 102.

ETSI EN 319 432 Protocol profiles for trust service providers providing AdES digital signature generation services

This document will specify protocol profiles for the format and procedures for TSPs providing signature generation services.

ETSI EN 319 442 Protocol profiles for trust service providers providing AdES digital signature validation services

This document will specify protocol profiles for the format and procedures for TSPs providing signature validation services.

Conformity Assessment

ETSI EN 319 403 Trust service provider conformity assessment - Requirements for conformity assessment bodies assessing trust service providers

This document contains requirements for the competence, consistent operation and impartiality of conformity assessment bodies assessing conformity of trust service providers to standardized criteria for the provision of trust services. Requirements and guidance set out in this document are independent of the class of trust service provided.

Testing Conformance & Interoperability

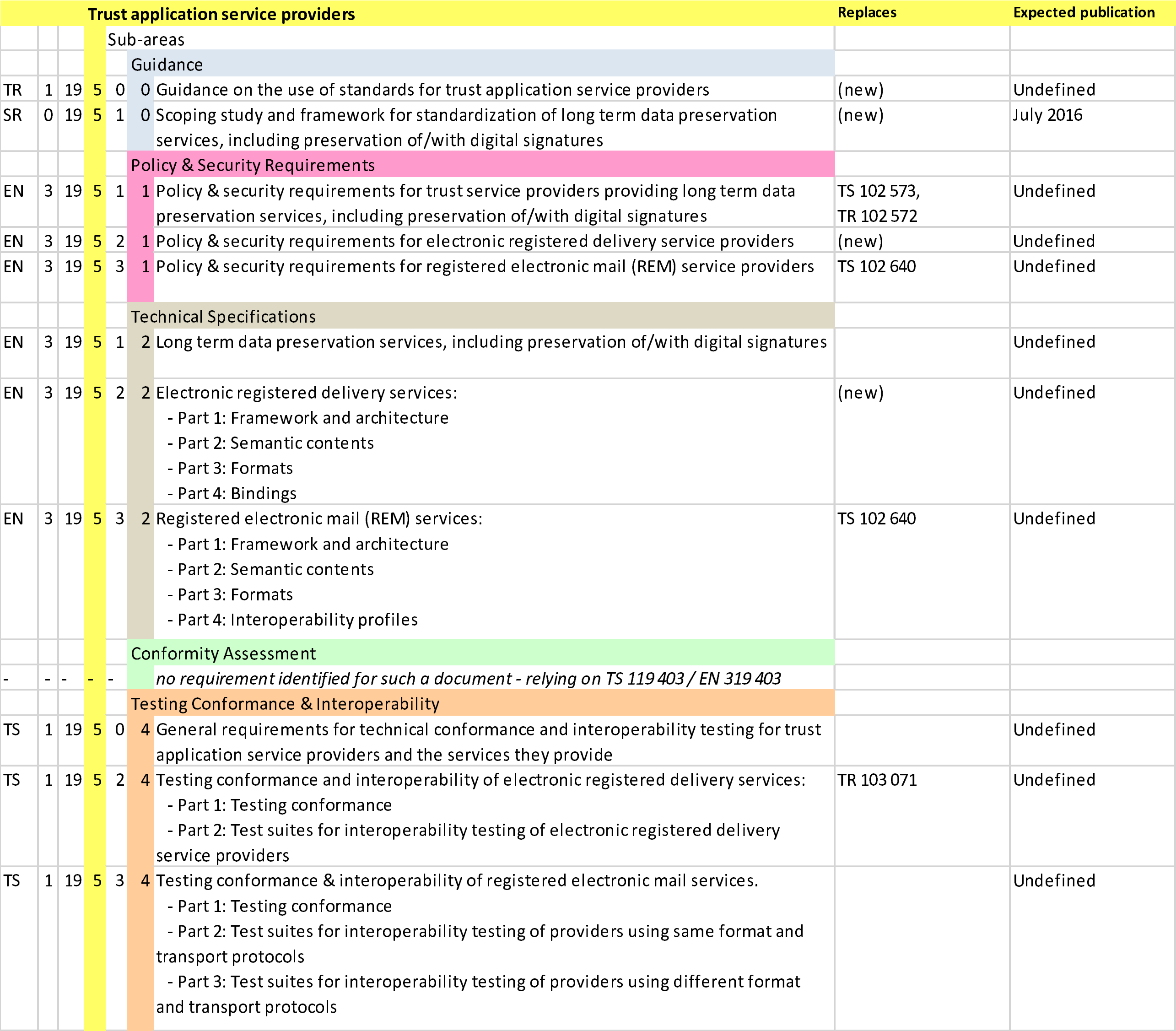
Not applicable so far.

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.

4.3.6 Trust application service providers

The documents for trust application service providers are summarized in table 6 with further details provided below.

Table 6: Standards for trust application service providers



						Trust application service providers	Replaces	Expected publication
				Sub-areas				
				Guidance				
TR	1	19	5	0	0	Guidance on the use of standards for trust application service providers	(new)	Undefined
SR	0	19	5	1	0	Scoping study and framework for standardization of long term data preservation services, including preservation of/with digital signatures	(new)	July 2016
				Policy & Security Requirements				
EN	3	19	5	1	1	Policy & security requirements for trust service providers providing long term data preservation services, including preservation of/with digital signatures	TS 102 573, TR 102 572	Undefined
EN	3	19	5	2	1	Policy & security requirements for electronic registered delivery service providers	(new)	Undefined
EN	3	19	5	3	1	Policy & security requirements for registered electronic mail (REM) service providers	TS 102 640	Undefined
				Technical Specifications				
EN	3	19	5	1	2	Long term data preservation services, including preservation of/with digital signatures		Undefined
EN	3	19	5	2	2	Electronic registered delivery services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Bindings	(new)	Undefined
EN	3	19	5	3	2	Registered electronic mail (REM) services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Interoperability profiles	TS 102 640	Undefined
				Conformity Assessment				
-	-	-	-	-		*no requirement identified for such a document - relying on TS 119 403 / EN 319 403*		
				Testing Conformance & Interoperability				
TS	1	19	5	0	4	General requirements for technical conformance and interoperability testing for trust application service providers and the services they provide		Undefined
TS	1	19	5	2	4	Testing conformance and interoperability of electronic registered delivery services: - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of electronic registered delivery service providers	TR 103 071	Undefined
TS	1	19	5	3	4	Testing conformance & interoperability of registered electronic mail services. - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of providers using same format and transport protocols - Part 3: Test suites for interoperability testing of providers using different format and transport protocols		Undefined

NOTE: Expected publication dates are provided for information and are subject to changes.

Guidance

ETSI TR 119 500 Guidance on the use of standards for trust application service providers

This document will provide guidance for the selection of standards for trusted application service providers for given business requirements. The following trust application services will be addressed: registered electronic delivery and registered electronic mail.

ETSI SR 019 510 Scoping study and framework for standardization of long term data preservation services, including preservation of/with digital signatures

This document will aim to specify the framework of standards for long term data preservation. ETSI SR 019 050 includes the sub-area of long term preservation within the area of trust application service providers.

Policy & Security Requirements

ETSI EN 319 511 Policy & security requirements for trust service providers providing long term data preservation services, including preservation of/with digital signatures

This document will specify policy and security requirements for trust service providers providing long term data preservation services, including preservation of/with digital signatures. Informative annexes will provide checklists for conformity assessment.

ETSI EN 319 521 Policy & security requirements for electronic registered delivery service providers

This document will define the policy requirements that are specific for electronic registered delivery providers required to be recognized as a provider of this type of services. It will define different conformance levels for each style of operation and the corresponding set of requirements to be satisfied in each level. It will reference ETSI EN 319 401 for generic requirements common to any trust service provider. Informative annexes will provide checklists for conformity assessment.

ETSI EN 319 531 Policy & security requirements for registered electronic mail (REM) service providers

This document will define policy requirements that are specific for REM service providers required to be recognized as a provider of this type of services. It will define different conformance levels for each style of operation and the corresponding set of requirements to be satisfied in each level. It will reference ETSI EN 319 401 for generic requirements common to any trust service provider, and ETSI EN 319 521 for common requirements of electronic registered delivery providers, of which REM service providers are a specific type. Informative annexes will provide checklists for conformity assessment.

Technical Specifications

ETSI EN 319 512 Long term data preservation services, including preservation of/with digital signatures

This document will specify technical specifications for services providing long term document and/or data preservation, including preservation of/with digital signatures. It also specifies the requirements on the use of digital signatures and time-stamping to maintain the authenticity and integrity of documents when stored over long periods.

ETSI EN 319 522 Electronic registered delivery services

This document will contain technical specifications for the provision of electronic registered delivery services. This will be a multi-part document. ETSI SR 019 050 contains the proposal for the contents of the different parts of ETSI EN 319 522. Below follows the list of parts, based on ETSI SR 019 050 proposals:

Part 1: **Framework and architecture:** It will provide an overview of the multi-part EN. It will also include an overall view of the standardized service, addressing at least the following aspects:

- Logical model, including an overview of the different entities, components and events involved in an electronic delivery transaction.
- Interfaces between the different roles and providers.
- Relevant events in the data object flows and the corresponding evidence.
- Trust building among providers pertaining to the same or to different administrative domains.

Part 2: **Semantic contents:** This will specify the semantic contents to be produced and managed in electronic registered delivery transactions. It will deal with:

- **Message delivery content**. Specifications of the semantic of the meta-information that will possibly be associated to the transmission of the payload.

- **Evidence and identification content**. Specifications of the set of evidence managed in the context of the service provision. The document will fully specify the semantics, the components, and the components' semantics for all the evidence. The document will also specify the content related to end user identity to be managed in the transactions.
- **Service discovery content**. Specifications of the information related to the identification of the remote electronic registered delivery management domain, the negotiation of capabilities and requirements that a service supports and the information related to the establishment of trust of a service (e.g. the content that will appear in an appropriate TSL extension for electronic registered delivery services).

Part 3: **Formats:** It will specify the formats for the different contents to be produced and managed in electronic registered delivery transactions. This part will deal with:

- **Message delivery formats**. Specifications of the format/formats for the meta-information specified by "Semantic contents" part. Meta-information could come either in attached (as an envelope including the payload) or detached format.
- **Evidence and identification formats**. Specifications of the syntax for the set of evidence and user identity information specified in "Semantic contents" part.
- **Service discovery formats**. Specifications of the format/formats for capabilities, requirements and trust information specified in the "Semantic contents" part.

Part 4: **Bindings:** This part will be itself split in sub-parts. Each part will fully specify the binding to a messaging protocol that is supporting electronic delivery services provision. The messaging protocols will be defined. This will include specification on how to transport evidence within the protocols messages, how to include signature's provider within the protocol's message, etc. Each part will specify anything that is required to ensure interoperability among providers of the service being compliant with that part. Each sub-part will deal with:

- **message delivery binding;**
- **evidence and identification binding;**
- **capability/requirements binding.**

ETSI EN 319 532 Registered Electronic Mail (REM) Services

This document will contain technical specifications for the provision of registered electronic mail. It will evolve the currently existing ETSI TS 102 640. The final EN will exclusively specify those aspects that are particular to the provision of electronic registered delivery services using SMTP and S/MIME as transport protocol and data formats respectively. This will be a multi-part EN. ETSI SR 019 050 contains the proposal for its contents:

Part 1: **Framework and architecture:** This part will provide an overview of the multi-part EN. It will normatively refer to ETSI EN 319 522 part 1 whenever applicable and will include aspects of the provision of registered electronic mail standardized services, which are not common to the provision of other types of electronic delivery provision, but specific to REM.

Part 2: **Semantic contents:** This part will specify semantic contents to be produced and managed in REM transactions. It will normatively refer to ETSI EN 319 522 part 2 whenever applicable and will specify semantics which are not common to the provision of other types of electronic delivery services, but specific to the provision of REM services.

Part 3: **Formats:** This part will specify the formats for the different messages to be produced and managed in REM transactions using S/MIME on SMTP. It will normatively refer to ETSI EN 319 522 part 3 whenever applicable and will specify issues which are specific to REM.

Part 4: **Interoperability profiles:** This part will contain sub-parts. Each one will specify profile(s) for seamless exchange of data objects across providers that use the same or different formats and/or transport protocols.

Conformity Assessment

Not applicable so far.

Testing Conformance & Interoperability

ETSI TS 119 504 General requirements for testing conformance & interoperability of trust application service providers

This document will specify general requirements for specifying technical conformance and interoperability testing for trust application service providers and the services they provide.

ETSI TS 119 524 Testing conformance & interoperability of electronic registered delivery services

This document will define test suites that support interoperability tests among entities providing electronic registered delivery services. It will also specify tests assertions for checking conformance against relevant specifications of ETSI EN 319 522. Below follows the list of parts based on ETSI SR 019 050 proposals:

Part 1: **Testing conformance:** This part will specify test assertions for checking conformance against relevant specifications of ETSI EN 319 522.

Part 2: **Test suites for interoperability testing of electronic registered delivery service providers:** This document will apply to those providers that implement the service provision using the same combination of format and transport protocols.

ETSI TS 119 534 Testing conformance & interoperability of registered electronic mail services

This document will define test suites that support interoperability tests among entities providing registered electronic mail services. It will also specify tests assertions for checking conformance against relevant specifications of ETSI EN 319 532. Below follows the list of parts based on ETSI SR 019 050 proposals:

Part 1: **Testing conformance:** This document will specify the tests to be performed for checking conformance against ETSI EN 319 532.

Part 2: **Test suites for interoperability testing of providers using same format and transport protocols:** This document will apply to those providers that implement the service provision using the same combination of format and transport protocols.

Part 3: **Test suites for interoperability testing of providers using different format and transport protocols:** This document will apply to 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.

4.3.7 Trust service status lists providers

Table 7: Standards for trust service status lists providers

			Trust service status lists providers				**Replaces**	**Expected publication**
				Sub-areas				
					Guidance			
TR	1	19	6	0	0	Guidance on the use of standards for trust service status lists providers	new	published
					Policy & Security Requirements			
TS	1	19	6	1	1	Policy & security requirements for trusted lists providers		Undefined
					Technical Specifications			
TS	1	19	6	1	2	Trusted lists	TS 102 231	published
					Conformity Assessment			
-	-	-	-	-		*no requirement identified for such a document - relying on TS 119 403 / EN 319 403*		
					Testing Conformance & Interoperability			
TS	1	19	6	1	4	Testing conformance & interoperability of trusted lists: - Part 1: Test suites for testing interoperability of XML representation of trusted lists. - Part 2: Specifications for testing conformance of XML representation of trusted lists	(new)	Undefined

NOTE: Expected publication dates are provided for information and are subject to changes.

Guidance

ETSI TR 119 600 Guidance on the use of standards 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

ETSI TS 119 611 Policy & security requirements for trusted list providers

This document will specify policy requirements for issuers of trusted lists in particular as they are defined in the applicable European legislation. This will build on the requirements in ETSI EN 319 401 when applicable.

Technical Specifications

ETSI TS 119 612 Trusted lists

This document contains the specifications related to trusted lists in particular as they are defined in the applicable European legislation.

NOTE 1: CD 2009/767/EC [i.18] amended by CD 2010/425/EU [i.19] and by CD 2013/662/EU [i.23] establishes the specifications for EU Member States trusted lists for their use in the context of Directive 1999/93/EC [i.1] and of the Services Directive 2006/123/EC [i.14]. Those specifications builds on version 1.1.1 of ETSI TS 119 612. CID (EU) 2015/1505 [i.26] specifies the format for trusted lists applicable for the purposes of eIDAS Regulation 910/2014/EU [i.21] building upon version 2.1.1 of ETSI TS 119 612.

NOTE 2: As conceptually trusted lists (TL) or trust service status lists (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.

Conformity Assessment

Not applicable so far.

Testing Conformance & Interoperability

ETSI TS 119 614 Test suites and tests specifications for technical conformance & interoperability testing of trusted lists

This document will first define test suites for supporting the organization of interoperability testing events where different applications managing trusted lists can check their actual interoperability. Additionally, it defines a complete set of test assertions for testing technical conformance of trusted lists against the relevant trusted lists technical specifications. This document will help implementers and will likely accelerate the development of tools for creating and issuing trusted lists.

Part 1: **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 ETSI TS 119 612.

Part 2: **Specifications for testing conformance of XML representation of trusted lists:** This document will specify test assertions for testing compliance of trusted lists against trusted list specifications. It would 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 would allow developing a tool that could automatically check that the trusted lists generated by a certain tool are fully conformant with the relevant aforementioned specifications.

Annex A:
TSP and CSP Concept

There has been confusion over the use of the term certification service provider (CSP) within the context of digital signatures and the need to also identify providers of trust services not relating to digital signatures. The present document proposes the use of the term trust service provider (TSP) to cover providers of electronic services that enhance 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 digital signatures, can encompass, when related to digital signatures:

a) TSPs supporting digital signatures and related services covering notably, as listed in clause 4.3.5, trust service providers issuing qualified and/or non-qualified certificates, time-stamping service providers, signature generation service providers, and signature validation service providers; and

b) Trust application service providers, i.e. TSP applying digital signatures for building added value trust services on top of digital signatures. These cover e.g. registered electronic mail (REM) or electronic registered delivery service providers, and information preservation service providers.

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

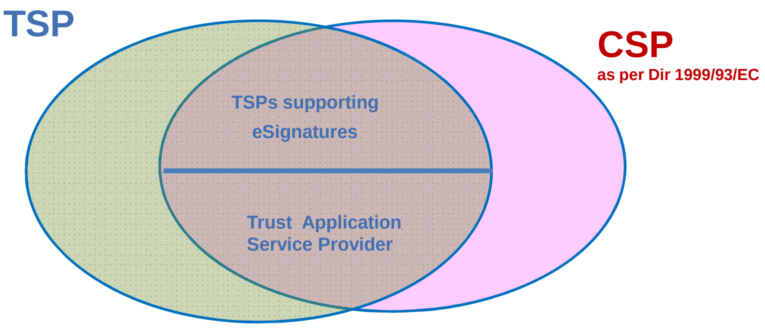


Figure A.1: Illustration of relationship between TSP and CSP

The term CSP as defined in Directive 1999/93/EC [i.1] is commonly used to cover electronic services to support signatures such as listed in clause 4.3.5.

However, this term CSP can also be used to describe non-electronic services supporting digital signatures such as providers of consulting services on signatures. Also, it is not clear whether services applying digital signatures, as listed in clause 4.3.6, are also examples of a CSP.

The term TSP is not restricted to TSPs supporting digital signatures (as addressed in clause 4.3.5) but also includes trust application service providers as listed in clause 4.3.6 as well as trust applications not employing digital signatures. For example TSP encompasses TSPs providing services for long-term preservation using secure storage instead of digital signatures.

Annex B: Bibliography

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.

History

Document history		
V1.1.1	September 2015	Publication
V1.2.1	April 2016	Publication