ETSI TR 119 400 V1.1.1 (2016-03)

Electronic Signatures and Infrastructures (ESI);
Guidance on the use of standards for trust service providers supporting digital signatures and related services

Reference
DTR/ESI-0019400

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

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

ETSI TR 119 000 [i.2] ("The framework for standardization of signatures: overview") provides an overview of the general structure for digital signatures standardization outlining existing and potential standards for such signatures. It identifies six areas of standardization with a list of existing and potential future standards in each area.

The present document is one of a series guidance documents to assist readers and their suppliers in identifying the digital signature standards, as well as technical specifications, and their options relevant to their needs. Each guide addresses a particular area as identified in ETSI TR 119 000 [i.2].

This series is based on the process of selecting business scoping parameters for each area of standardization. The selection of these scoping parameters is based on process involving an analysis of the business requirements and associated risks leading to an identification of the policy and security requirements and to an analysis of the resulting business scoping parameters from which the appropriate standards and options can be selected. From the requirements expressed in terms of business scoping parameters for an area, each guidance document provides assistance in selecting the appropriate standards and their options for that area. Where standards, as well as technical specifications, and their options within one area make use of another area this is stated in terms of scoping parameters of that other area.

A trust service is a service which enhances the trust and confidence in electronic transactions between parties. They are used, for example, to certify ownership of keys used for digital signatures. The present document does not include any normative requirements but provides guidance on addressing the trust service provider (TSP) supporting digital signatures, on the selection of applicable standards and their options for a particular business implementation context and associated business requirements.

This general process of the selection of standards and options is described further in ETSI TR 119 000 [i.2], clause 4.2.6.

1 Scope

The present document provides guidance on the selection of standards and options for the trust service provider supporting digital signatures and related services (area 4) as identified in ETSI TR 119 000 [i.2].

The present document describes the business scoping parameters relevant to this area (see clause 5) and how the relevant standards and options for this area can be identified given the business scoping parameters (see clause 6).

The target audience of the present document includes:

1) Business managers who potentially require support from digital signatures and in particular the provision of related supporting trust services in their business will find here an explanation of how digital signatures standards can be used to meet their business needs.

2) Application architects who will find here material that will guide them throughout the process of designing a system that fully and properly satisfies all the business and legal/regulatory requirements specific to digital signatures and in particular the provision of related supporting trust services. They will gain a better understanding on how to select the appropriate standards to be implemented and/or used.

3) Developers of the systems who will find in the present document an understanding of the main reasons that lead the systems to be designed as they were, as well as a proper knowledge of the standards that exist in the field and that they need to know in detail for a proper development.

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 https://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] 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 and repealing Directive 1999/93/EC.

[i.2] ETSI TR 119 000: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview".

[i.3] ETSI TR 119 100: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation".

[i.4] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General policy requirements for trust service providers".

[i.5] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.6] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.7] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[i.8] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[i.9] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons".

[i.10] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for certificates issued to legal persons".

[i.11] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate Profile for web site certificates".

[i.12] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.13] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[i.14] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.15] ETSI EN 319 122 (all parts): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures".

[i.16] ETSI EN 319 132 (all parts): "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures".

[i.17] ETSI EN 319 142 (all parts): "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures".

[i.18] ETSI EN 319 162 (all parts): "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC)".

[i.19] ISO 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.20] Recommendation ITU-T X.509/ISO/IEC 9594-8: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.21] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[i.22] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.23] ETSI SR 019 020: "The framework for standardization of signatures; Standards for AdES digital signatures in mobile and distributed environments".

[i.24] ETSI TR 119 500: "Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for trust application service providers".

[i.25] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.26] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates".

[i.27] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[i.28] ISO/IEC 27002: "Information technology -- Security techniques -- Code of practice for information security management".

[i.29] IETF RFC 5816: "ESSCertIDv2 Update for RFC 3161".

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.25] and the following apply:

EU qualified trust service provider: trust service provider that meets the requirements for qualified trust service providers laid down in Regulation (EU) No 910/2014 [i.1]

NOTE: These definitions are aligned with those used in the standards referred to in the present document.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 119 001 [i.25] and the following apply:

CA Certification Authority
SSL Secure Socket Layer

NOTE: Newer version of this protocol has been specified as TLS [i.22].

TLS Transport Layer Security

4 Introduction to trust services and trust service providers

4.1 What is a trust service and trust service provider

A trust service is a service which enhances the trust and confidence in electronic transactions between parties. A trust service is provided by a "third" party (trust service provider - TSP) which needs to be trusted (directly or indirectly) by the transacting parties. The TSP provides information (e.g. a key that may be used to authenticate an identified person), in the form of a trust service token which can be used by the transacting parties to enhance the security of transactions between them. Generally, a TSP also provides associated management services to maintain information used in the trust service tokens.

The concept of TSP is a generalization of an earlier concept of a provider of public key certificates, commonly called a certification authority.

The concept of trust service and trust service provider is also used in relation to specific regulatory requirements in the European Union Regulation (EU) No 910/2014 [i.1] on electronic identification and trust services. This Regulation identifies a special class of trust service provider, called a "qualified trust service provider", which meets specific functional and security requirements. Other forms of qualified trust service provider may exist in other regulatory environments but the standards for qualified trust service providers identified in the present document are aimed at the EU Regulation and so are referred to as EU qualified trust service providers.

It is recognized that TSPs generally will operate in an international context and so not only need to meet EU Regulatory requirements but also need to address requirements for trust services as laid down by international fora such as the CA Browser Forum [i.26] and [i.27]. Thus, the standards for EU qualified trust services providers are defined as enhancements to the general requirements for trust service providers which are compatible with the international requirements such as specified by the CA Browser Forum.

Standards identified in the present document are applicable to both EU qualified trust service providers as well as trust service providers operating in an international context, and are aimed for use in both regulated and non-regulated environments.

4.2 Types of trust service provider

4.2.1 TSP issuing certificates

One of the most commonly known form of TSP is a certification authority (CA). A certification authority is a TSP which issues a public key certificate (also called certificate). A public key certificate binds the public key of one transacting party with other information about the party including its identity. Such a certificate can be used to authenticate the origin of data protected using the associated private key or to validate a digital signature created using the associated private key. Different classes of certificates can be used to provide alternative levels of legal compliance (e.g. qualified or not) and certify different forms of identity (e.g. natural person, legal person).

Regulation (EU) No 910/2014 [i.1] identifies a special class of (public key) certificate, called "qualified" certificate, which meets given functional and security requirements. This is referred to in the standards identified in the present document as an "EU qualified certificate". Under this regulation different types of EU qualified certificates are defined, namely for electronic signatures, for electronic seals and for web site authentication.

As with other standards identified in the present document the requirements for EU qualified certificates and EU qualified trust service providers are based on internationally recognized standards in particular those published by the CA Browser Forum [i.26] and [i.27].

The standards for TSPs identified in the present document particularly address the requirements of TSP issuing certificates to support:

a) Digital signatures (that can be used to implement advanced electronic signatures and advanced electronic seals as they are defined in Regulation (EU) No 910/2014 [i.1]). These certificates are designed for use with the CadES [i.15], XadES [i.16], PadES [i.17] digital signature formats and AsiC [i.18] containers;

b) Web site authentication TLS [i.22] or the earlier SSL equivalent meeting CA Browser Forum requirements specified in [i.26] and [i.27].

4.2.2 TSP issuing time-stamps

Another form of trust service is a time-stamping service. A time-stamping service provider issues time-stamps which can be used to prove the existence of given data at a particular time. This can be used to:

- Enhance the security of digital signatures (such as defined in CadES [i.15], XadES [i.16], PadES [i.17] and as incorporated in AsiC [i.18]). Time-stamps are used in the augmented levels of the AdES formats, firstly to provide additional evidence of the time when a signature had been created, secondly to extend the life-time of digital signatures when applied, for example, to archived documents.

- Protect the authenticity and integrity of documents and other data. Time-stamping a document can ensure that any change to a document can be detected, and provide evidence that the document existed at a given time.

4.2.3 Other potential trust services

Other classes of trust services have been identified that are relevant to this area of the framework for standardization of signatures. This in particular includes:

- Signature generation services: Trusted services that can be used to generate digital signatures for remote users (see ETSI SR 019 020 [i.23]).

- Signature validation services: Trusted services that can be used to confirm the technical validity of a digital signature (see ETSI SR 019 020 [i.23]).

NOTE: Signature generation and validation services are currently not addressed in the present document.

4.2.4 Other trust services outside scope

The scope of the present document is limited to those trust services supporting digital signatures and web site authentication. However, some of the standards referred to in the present document (e.g. ETSI EN 319 401 [i.4] and ETSI EN 319 403 [i.14]) can be applied to other trust services including trust services applying digital signatures such as e-delivery services (see ETSI TR 119 500 [i.24]).

5 Aspects of trust services requiring standardization

5.1 Policy & security requirements

In order to ensure the trustworthiness of a TSP's service it is important that it is provided in a way that the security and business practices of the TSP meet the recognized best practices for such services, and in the case of EU qualified TSPs also meet the requirements laid out in the applicable legislation. Any weaknesses in the TSP practices can potentially lead significant risk of compromise to the TSP's services and so break the trust that the TSP users have in being able to ensure the security of their own transactions based on the TSP's services.

Through standardization of such best practices there is a recognized level of trust on which the users can base their decision to use the services of a TSP. These standards are described in terms of the requirements on TSP's policies and practices, and include standard trust service policy identifiers which can be used to identify the specific policy requirements applicable to a given trust service token (e.g. standard certificate policy for EU qualified certificates supporting digital signatures).

A TSP service makes use of system components (e.g. cryptographic devices, computer systems) which need to be secure for the overall operation of the TSP service to be secure. The security of such system components is commonly assured through evaluation criteria which define the security functions of the system components and assurance techniques that are expected to assure their security. General standards for such evaluation criteria are specified in ISO 15408 [i.19]. Standards based on ISO 15408 [i.19] define the evaluation criteria specific to one type of device or system.

5.2 Certificate and time-stamp profiles

The main function of a TSP is to provide a data object, called a trust service token, which can be used to secure transactions between parties who are users. The trust service token most widely used in support of digital signatures and web site authentication is a public key certificate (commonly called a certificate) which binds an identity with a key used to authenticate one transacting party to another. Another trust service token is a time-stamp which binds a time to a particular data object or document.

For the TSP to produce trust service tokens (e.g. certificate or time-stamps) to be used by transacting parties the tokens need to be provided in a form which meets their needs for securing transactions. The trust service tokens need to include the required information and be encoded in a way that is understood by the transacting parties. General standards exist for the main forms of trust service tokens: X.509 [i.20] for certificates and IETF RFC 3161 [i.21] (updated by IETF RFC 5816 [i.29]) for time-stamps. However, these standards include a number of elements which can be used in a variety of manners, and options which may not be available from the TSP although considered necessary by the transacting parties.

In order to maximize interoperability between TSPs and the transacting parties, specific choices often need to be made on options that commonly exists in standards. Further standardization is often needed to specify the specific elements of the "base" standards (e.g. X.509 [i.20] or IETF RFC 3161 [i.21] updated by IETF RFC 5816 [i.29]) which are relevant to particular usage (e.g. EU qualified certificates for electronic signatures of natural persons). Such standards are called "profiles".

5.3 Conformity assessment

In order to gain assurance that a TSP's service applies the best practices expected for it to be trustworthy, the TSP needs to be checked that its policies and practices meet the standard criteria for its services. This is done through an independent body assessing whether the TSP's policies and practices meet the requirements laid out in the standard criteria, and that the policies and practices are being effectively applied. This independent body is called a conformity assessment body, and employs auditors to visit the TSP regularly to check that the standard criteria are being met.

Conformity assessment standards lay out the required capabilities of the conformity assessment body and how the assessment is carried out.

A similar process is defined for assessing systems and devices based on the common criteria (ISO 15408 [i.19]). This assessment is also carried out by a conformity assessment body but working in assessment laboratories where the device being assessed is checked out.

Such conformity assessment generally is required to get formal recognition of the trustworthiness of the TSP by:

- a legal entity, such as a "supervisory" body as identified in Regulation (EU) No 910/2014 [i.1], concerned with regulating the operation of TSPs;
- by a commercial or governmental organization, which can use the services of a TSP; or
- a commercial association, such as the CA Browser Forum, which represents the interests of a community of users.

5.4 Testing technical conformance and interoperability

The interoperability and conformance to technical standards, of trust service tokens produced by TSPs is an element of the general interoperability of digital signatures. Thus any interoperability or conformance test on trust services and trust service tokens is carried out as part of a wider digital signature interoperability test as described in ETSI TR 119 100 [i.3].

6 Selection process

6.1 Basis for selection of standards

The process of selecting the appropriate standards and options as identified in ETSI TR 119 000 [i.2] clause 4.2.6 is applied to the TSP area as follows.

1) The basic characteristics of the trust service need to be identified. With the currently defined standards for trust services this can include:

   a) TSP support for digital signatures (such as defined in CadES [i.15], XadES [i.16], PadES [i.17] and as incorporated in AsiC [i.18]). This requires TSP issuing certificates, and can require TSP issuing time-stamps (see 2 below).

   b) TSP support for web site authentication, based on the Transport Layer Security protocol [i.22] or equivalent protocol for securing access to web services. This requires TSP issuing certificates.

   c) TSP support for archival documents and other data, independent of whether they are signed or not, through use of time-stamping. This requires TSP issuing time-stamps.

NOTE 1: The detailed use of TSP issuing time-stamps for archival is subject to ongoing standardization.

NOTE 2: The use of TSPs for issuing certificates to support electronic identities, or to certify other attributes of person, independent of digital signatures, time-stamping or web services is outside the scope of standards referenced in the present document.

2) If the requirement is for support of digital signatures, the analysis of the business requirements for TSP issuing certificates and TSP issuing time-stamps should be based on the requirements of the customers (or business partners) of a TSP. Customer requirements for certificates (qualified or otherwise) for digital signatures and time-stamps can be derived from the guidance given in ETSI TR 119 100 [i.3]. In particular, the business scoping parameters should be taken into account as follows:

   - **Legal effect of signature:** Whether the business process requires a specific type of digital signature, e.g. a qualified electronic signature / seal implying the need for a "qualified certificate", or another more general purpose public key certificate needed to support an advanced electronic signature as defined in the applicable legislation.

   - **Timing and sequencing:** Whether the timing and sequencing requirements imply the need for time-stamp tokens before the signature or as part of a signature (i.e. as a signature time-stamp).

- **Longevity and resilience to change:** Whether the requirements relating to the length of time that signed information may be kept may imply, for example, the need for time-stamps.

3) Based on the legal effect of the signature (see 2) above) or legal requirement for authentication of the web site the TSP will require to be EU Qualified (i.e. fulfilling the requirements of qualified trust services as defined in Regulation (EU) No 910/2014 [i.1]) or just fulfilling the general requirements for good practice for trust services.

4) If TSP issuing certificates is required, it is necessary to establish whether the certificate identifies a natural or legal person.

6.2 Business scoping parameters for TSP standards

In selecting the appropriate TSP standards and options within standards, some parameters of the business requirements need to be identified. These are referred to in the present document as business scoping parameters.

From the above analysis the following business scoping parameters need to be identified, called business scoping parameters, to facilitate the selection of the appropriate standards as described in the following clause. The basic business scoping parameters are:

a) Whether the TSP is to have legal effect EU qualified or has other general recognized security level for good TSP practices.

b) The trust service required:

   i) TSP issuing certificate; or

   ii) TSP issuing time-stamp.

c) If TSP issuing certificates, whether the certificate identifies:

   i) Natural person; or

   ii) Legal person and organizations.

d) If TSP issuing certificate whether the certificate is for:

   i) Digital signature; or

   ii) Web site authentication.

7 Selecting the most appropriate standards

The standards for TSP services covered by the present document should be selected based on the business scoping parameters as described in clause 6 as follows:

a) The relevant "policy requirements" document should be selected for the type of TSP service (issuing certificates or time-stamps), and legal effect of service (EU Qualified or general):

   i) If TSP issuing certificates and general legal effect is required, then ETSI EN 319 411-1 (General policy and security requirements for TSP issuing certificates) [i.5] should be selected. This applies to both certificates for digital signature and web site authentication.

NOTE 1: ETSI EN 319 411-1 [i.5] references requirements from ETSI EN 319 401 [i.4] (General policy requirements for TSPs), the CA Browser Forum baseline [i.27] and extended validation [i.26] guidelines.

   ii) If TSP issuing certificates and EU Qualified legal effect is required, then ETSI EN 319 411-2 [i.6] (Policy and security requirements for TSP issuing EU qualified certificates) should be selected. This applies to both certificates for digital signature and web site authentication.

NOTE 2: ETSI EN 319 411-2 [i.6] references requirements from ETSI EN 319 411-1 [i.5].

   iii) If TSP issuing time-stamps is required (EU Qualified or general legal effect), then ETSI EN 319 421 [i.7] should be selected.

NOTE 3: All the above "policy requirements" standards reference requirements from ETSI EN 319 401 [i.4] (General policy requirements for TSPs). ETSI EN 319 401 [i.4] references recommended requirements from ISO/IEC 27002 [i.28].

b) The relevant certificate or time-stamp profile should be selected for the type of service (issuing certificates or time-stamps), legal effect and, for TSP issuing certificates, the type of identity be certified:

NOTE 4: The above "policy requirements" documents require the relevant certificate or time-stamp profile and so the following references will be implied through reference to the appropriate policy and selection of options within the referenced document.

i) If TSP issuing certificates for digital signatures for natural persons (whether EU Qualified or general legal effect), then ETSI EN 319 412-2 [i.9] (Certificate profile for certificates issued to natural persons) should be selected.

ii) If TSP issuing certificates for digital signatures for legal persons (whether EU Qualified or general legal effect), then ETSI EN 319 412-3 [i.10] (Certificate profile for certificates issued to legal persons) should be selected.

iii) If TSP issuing certificates for web sites (whether EU Qualified or general legal effect, natural or legal person), then ETSI EN 319 412-4 [i.11] (Certificate profile for web site certificates) should be selected.

iv) If any TSP issuing certificates is required to be EU Qualified, then ETSI EN 319 412-5 [i.12] (QCStatements) should be selected.

NOTE 5: ETSI EN 319 412 parts 2 [i.9], 3 [i.10] or 4 [i.11] reference requirements from part 5 when the certificate is to be EU Qualified.

v) If TSP issuing time-stamps (whether EU Qualified or general), then ETSI EN 319 422 [i.13] (Time-stamping protocol and time-stamp token profiles) should be selected.

c) Any trust service should be audited by a conformity assessment body which complies with ETSI EN 319 403 [i.14].

This is summarized in table 1 with the appropriate standard indicated by an "X".

Table 1: selection of standards

Standard	Topic	Business scoping parameters									
		Issuing certificate								Issuing time-stamp	
		General				EU Qualified				General	EU Qualified
		Natural		Legal		Natural		Legal			
		Dig Sig	Web Site	Dig Sig	Web Site	Dig Sig	Web Site	Dig Sig	Web Site		
ETSI EN 319 401 [i.4] (see note 1)	General policy requirements for TSPs	X	X	X	X	X	X	X	X	X	X
ETSI EN 319 411-1 [i.5]	General policy and security requirements for TSP issuing certificates	X	X	X	X	X	X	X	X		
ETSI EN 319 411-2 [i.6]	Policy and security requirements for TSP issuing EU qualified certificates					X	X	X	X		
ETSI EN 319 421 [i.7]	Policy and security requirements for TSPs issuing time-stamps									X	X

Standard	Topic	Business scoping parameters									
		Issuing certificate								Issuing time-stamp	
		General				EU Qualified				General	EU Qualified
		Natural		Legal		Natural		Legal			
		Dig Sig	Web Site	Dig Sig	Web Site	Dig Sig	Web Site	Dig Sig	Web Site		
ETSI EN 319 412-2 [i.9] (see note 3)	Certificate profile for certificates issued to natural persons	X				X					
ETSI EN 319 412-3 [i.10] (see note 3)	Certificate profile for certificates issued to legal persons			X				X			
ETSI EN 319 412-4 [i.11] (see note 3)	Certificate profile for web site certificates		X		X		X		X		
ETSI EN 319 412-5 [i.12] (see note 3)	QCStatements					X	X	X	X		
ETSI EN 319 422 [i.13]	Time-stamping protocol and time-stamp token profiles									X	X
ETSI EN 319 403 [i.14] (see note 2)	TSP Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers	X	X	X	X	X	X	X	X	X	X

NOTE 1: ETSI EN 319 401 [i.4] is incorporated by reference in the other policy requirements documents (i.e. ETSI EN 319 411-1 [i.5] and ETSI EN 319 411-2 [i.6] and ETSI EN 319 421 [i.7]). ETSI EN 319 401 [i.4] can be used as the basis for any TSP policy requirement specification, regardless of the trust service provided, including trust application service providers (see ETSI TR 119 500 [i.24]).

NOTE 2: The standard ETSI EN 319 403 [i.14] can be used for third party audit meeting regulatory requirements for conformity assessment (e.g. as specified in article 20.1 of Regulation (EU) No 910/2014 [i.1]) and to assure that a TSP meets the requirements of application providers which depend on the use of trust services provided by a TSP (as specified by CA Browser Forum [i.26], [i.27]). In addition, ETSI EN 319 403 [i.14] can be used for conformity assessment of TSPs other than those supporting digital signature including trust application service providers as described in ETSI TR 119 500 [i.24].

NOTE 3: ETSI EN 319 412-1 [i.8] provides an overview of the different other parts of ETSI EN 319 412-2 [i.9], ETSI EN 319 412-3 [i.10], ETSI EN 319 412-4 [i.11] and ETSI EN 319 412-5 [i.12] and specifies common data structures used in those parts.

The relationship between the standards identified above is illustrated by figure 1.

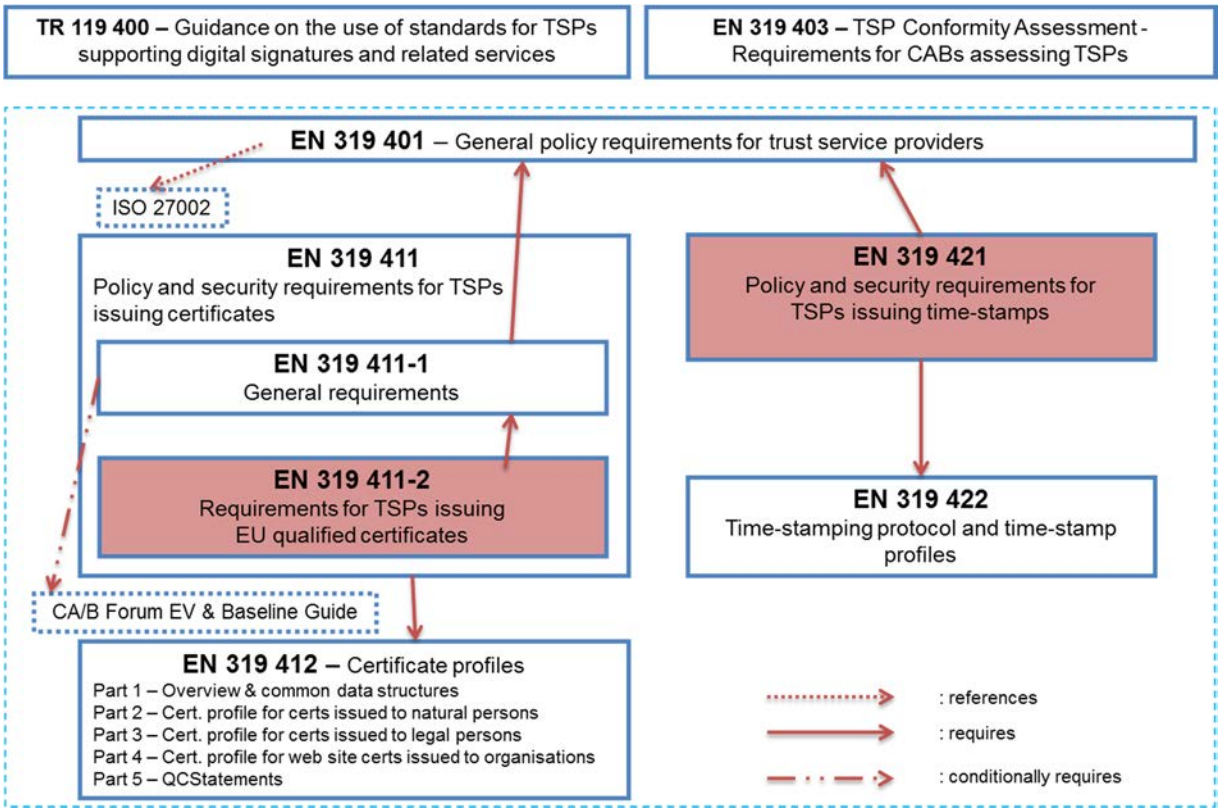

Figure 1: Relationships between standards

Annex A:
Clarification of requirements in TSP Standards

The following clarification can be considered in applying standards for trust service providers supporting digital signatures and related services.

ETSI EN 319 401 [i.4], clause 7.13 b)

This clause requires that a TSP's services be made accessible to persons with disabilities. In line with European Union Regulation (EU) No 910/2014 [i.1] article 15 it is the intention that this clause be applied "where feasible".

History

Document history		
V1.1.1	March 2016	Publication