# ETSI TR 119 600 V1.1.1 (2015-05)


**Electronic Signatures and Infrastructures (ESI);**
**Business guidance**
**for trust service status lists providers**

Reference
DTR/ESI-0019600

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 (http://ipr.etsi.org).

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

# Foreword

This 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

Trust service status list is the general term used to designate the form of a signed list as the basis for presentation of trust service status information. The purpose of a trust service status list is to provide a harmonized way in which approval schemes, having an oversight role with regards to trust services and their providers, can publish information about the services and trust service providers which they currently oversee, or indeed (through the provision of historical information) have overseen.

# 1 Scope

The present document provides guidance on the selection of standards and their options to organizations wishing to establish a trust service status list, for a particular business implementation context and associated business requirements.

The present document describes the business scoping parameters relevant to this area and how the relevant standards and options for this area can be identified given these business scoping parameters.

The target audience of the present document includes those potentially requiring support from trust services and in particular trust service status lists. The present document provides an explanation of how related standards can be used to meet the business needs.

# 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.

NOTE: This Directive and its implementations in EU Member States legislation are the applicable European legislation until 1 July 2016 at which date the Directive will be repealed by Regulation (EU) No 910/2014 [i.2].

[i.2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.3] ETSI TS 119 612 (V1.1.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

[i.4] 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.5] ETSI EN 319 411: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates".

[i.6] European Regulation 765/2008 of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

[i.7] 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.8] 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.9] ETSI TS 102 231: "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.10] ETSI TS 119 611: "Electronic Signatures and Infrastructures (ESI); Policy & security requirements for trusted lists providers".

[i.11] ETSI TS 119 602: "Electronic Signatures and Infrastructures (ESI); Trust service status lists".

[i.12] ETSI TS 119 172: "Electronic Signatures and Infrastructures (ESI); Signature policies".

[i.13] ETSI TS 119 603: "Electronic Signatures and Infrastructures (ESI); General requirements and guidance for conformity assessment of trust service status lists providers".

[i.14] ETSI TS 119 613: "Electronic Signatures and Infrastructures (ESI); Requirements for conformity assessment bodies assessing trusted lists providers".

[i.15] ETSI TS 119 614: "Electronic Signatures and Infrastructures (ESI); Testing conformance & interoperability of trusted lists".

# 3 Definitions and abbreviations

## 3.1 Definitions

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

**advanced electronic signature:** As defined in Directive 1999/93/EC [i.1].

**(digital) signature:** data associated to, including a cryptographic transformation of, a data unit that:

a) allows to prove the source and integrity of the data unit;

b) allows to protect the data unit against forgery; and

c) allows to support signer non-repudiation of signing the data unit.

**electronic signature:** As defined in Directive 1999/93/EC [i.1].

**trusted list:** list that provides information about the status and the status history of the trust services (including certification services) from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation

NOTE 1: In the context of EU MS, and as further specified by Commission Decision 2009/767/EC [i.4] as amended by Commission Decision 2010/425/EU [i.7] and Commission Decision 2013/662/EU [i.8], it refers to a European Union Member States supervision/accreditation status list of trust services from trust service providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC [i.1].

In the context of non-EU countries or international organizations, it refers to a list meeting the requirements of ETSI TS 119 612 [i.3] and providing assessment scheme based approval status information about trust services from trust service providers, for compliance with the relevant provisions of the applicable approval scheme and the relevant legislation.

NOTE 2: A trusted list is a specific type of trust service status list.

**trusted list provider:** entity which establishes, maintains and publishes trusted lists

NOTE: A trusted list provider is also called a trusted list issuer or a trusted list scheme operator (TLSO).

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

**trust service provider:** entity which provides one or more trust services

NOTE: This term includes and is used with a broader application than the term certification service provider (CSP) used in Directive 1999/93/EC [i.1].

**trust service status list:** form of a signed list as the basis for presentation of trust service status information

**trust service status list provider:** entity which establishes, maintains and publishes trust service status lists

NOTE: A trust service status list provider is also called a trust service status list issuer or a trust service status list scheme operator (TSLSO).

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

EXAMPLE: Certificates, CRLs, time stamps, OCSP responses. Physical tokens can be devices on which binary objects (tokens or credentials) are stored. Equally, a token can be the performance of an act and the generation of an electronic record, e.g. an insurance policy or share certificate.

## 3.2 Abbreviations

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

| | |
|---|---|
| CA | Certification Authority |
| CD | Commission Decision |
| CSP | Certification Service Provider |
| EC | European Commission |
| EEA | European Economic Area |
| EU | European Union |
| EUMS | European Union Member States |
| IPR | Intellectual Property Rights |
| LOTL | List Of Trusted Lists |
| MS | Member State |
| TL | Trusted List |
| TLSO | Trusted List Scheme Operator |
| TR | Technical Report |
| TS | Technical Specification |
| TSL | Trust service Status List |
| TSLSO | Trust service Status List Scheme Operator |
| TSP | Trust Service Provider |
| XML | eXtensible Markup Language |

# 4 Introduction to trusted lists, trust services status lists and their providers

## 4.1 Trust service and trust service provider

A trust service is defined as an electronic service which enhances trust and confidence in electronic transactions (typically, but not necessarily, using cryptographic techniques or involving confidential material). A trust service is provided by a "third" party, so called a trust service provider (TSP), which needs to be trusted (directly or indirectly) by the transacting parties. As part of its trust service, the TSP provides a specific trust service output, a so-called 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.

Trust services can be of different nature, the most common ones are the provision of public key certificates, time-stamping services, signature generation services, signature validation services, registered electronic mail services, long term preservation of electronic digital signatures or secure archiving services.

Trust service providers can also provide complex trust services making use of digital signatures and potentially built on the combination of the above listed services.

The value of trust services and of the trust service tokens they result in is mainly dependent on the level of assurance and trust relying parties can place in them and in their providers which is in turn dependent on the level of security and quality of the policies and practices implemented by the trust service provider to provide them.

Different policies can be defined either in the context of the standardization (e.g. lightweight certificate policies, normalized certificate policies, extended normalized certificates as defined in ETSI EN 319 411 [i.5]) or according to specific sets of requirements and associated approval schemes defined by national legislations, communities or organizations. Such approval scheme operators are then facing the issue of defining or adopting a format and process for publishing approval status information with regards to the trust services and trust service providers against which the approval process has been conducted.

Such approval processes can be conducted by the approval scheme operator or rely on external assessments conducted by conformity assessment bodies whose capacity to conduct such assessment can in turn be the target of some approval process like an accreditation by a national accreditation body (e.g. as ruled out by European Regulation 765/2008 [i.6]) or simply be recognized by the approval scheme operator.

## 4.2 Trust service status lists and trusted lists

### 4.2.1 Trust service status lists

Trust service status list (TSL) is the general term used to designate the form of a signed list as the basis for presentation of trust service status information. The purpose of a trust service status list is to provide a harmonized way in which approval schemes, having an oversight role with regards to trust services and their providers, can publish information about the services and TSPs which they currently oversee, or indeed (through the provision of historical information) have overseen. An assessment scheme operator can also use the TSL to only refer to other assessment schemes, i.e. other TSLs. TSLs are based upon the reasoning that they will enhance the confidence of parties relying on trust services if these parties had access to information that would allow them to know whether a given TSP was operating under the approval of any recognized scheme at the time of providing their services and of any dependent transaction that took place.

### 4.2.2 Trusted lists

Trusted lists (TLs) are trust service status lists that provide information about the status and status history of the trust services from trust service providers (TSPs) regarding compliance with the relevant provisions of the applicable legislation on signatures and trust services for electronic transactions.

Trusted lists as established in the European Union by Commission Decision 2009/767/EC [i.4] as amended by Commission Decision 2010/425/EU [i.7] and Commission Decision 2013/662/EU [i.8], aim primarily at supporting the validation of qualified electronic signatures and advanced electronic signatures supported by a qualified certificate in the meaning of Directive 1999/93/EC [i.1]. They include, as a minimum, trust service providers supervised/accredited for issuing qualified certificates. Member States, as trusted list providers, can however additionally include in their national trusted list other types of approved trust service providers. Hence, trusted lists would also facilitate the cross-border use of a number of additional electronic trust services based on advanced electronic signatures, provided that the supporting trust services (e.g. issuing of non-qualified certificates) are part of the nationally supervised/accredited services and listed accordingly in the national trusted list.

TLs enable in practice any interested party to determine whether a trust service is or was operating in compliance with relevant requirements, currently or at some time in the past (e.g. at the time the service was provided, or at the time at which a transaction reliant on that service took place). In order to fulfil this requirement, trusted lists contain information from which it can be established whether the TSP's service is, or was, known by the trusted list provider and if so the status of the service. Trusted lists therefore contain not only the service's current status, but also the history of its status.

In order to validate that an advanced e-signature is supported by a qualified certificate in the context of Directive 1999/93/EC [i.1], a receiving party needs to check the trustworthiness of the qualified status of the certificate and that it has been issued by a trust service provider supervised to issue qualified certificates, as required by article 3.3 of Directive 1999/93/EC [i.1]. The trusted lists provide the receiving party with such necessary information about the related certification service having issued the qualified certificate, when listed as a legitimate service, its status and status history and potentially additional relevant information assisting the receiving party in validating the signature. The receiving party can also verify whether the signature is supported by a secure signature creation device as defined in Directive 1999/93/EC [i.1].

In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission publishes a central list with links to the locations where the trusted lists are published as notified by Member States. This central list, called the list of trusted lists (LOTL), is available in both a human readable format and in a format suitable for automated (machine) processing XML.

NOTE 1: The LOTL can be accessed from https://ec.europa.eu/digital-agenda/en/news/eu-trusted-lists-certification-service-providers.

Current version of Commission Decision 2009/767/EC [i.4], as amended by Commission Decision 2010/425/EU [i.7] and Commission Decision 2013/662/EU [i.8], refers to ETSI TS 119 612 [i.3] for specifying the technical format and operations on TLs.

NOTE 2: Regulation (EU) No 910/2014 [i.2] provides a constitutive value to trusted lists to provide information about the qualified status and status history of the trust services from trust service providers (TSPs) regarding compliance with the relevant provisions of the Regulation. It also extends the scope of TLs to other types of trust services than those consisting in the issuance of qualified certificates, namely to the qualified provision of qualified time-stamping services, qualified signature validation services, qualified electronic delivery services, qualified long term preservation of qualified electronic signatures. However until 1 July 2016 at which date it will be repealed by Regulation (EU) No 910/2014 [i.2], Directive 1993/99/EC [i.1], its implementations in EU Member States legislation and CD 2009/767/EC [i.4] as amended are the applicable European legislation.

Specifications of trusted lists as defined in ETSI TS 119 612 [i.3] can also be used by approval scheme operators from countries outside the European Union and the EEA countries or in the context of international organizations, to issue their own list that provides information about the status and status history of the trust services from Trust Service Providers (TSPs) they approve in their domains, e.g. in compliance with the relevant provisions of the applicable legislation and/or in compliance with those domains approval scheme. The benefits from the adoption of the same technical specifications than for EU MS trusted lists by non-EU countries or international organizations to issue their own lists are twofold:

1) This can be used to enable in practice any interested party to determine whether a trust service from a non-EU country or an international organization is or was operating under an approval scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place.

2) This can facilitate the declaration of mutual recognition between trust services and their outputs (e.g. between EU and other nations/organizations outside the EU, within or between groups of nations/organizations outside the EU).

NOTE 3: Hereafter the terms "non-EU countries" will be used to refer to countries outside the European Union and the EEA countries.

Trusted lists have four major components, in a structured relationship. These components are information:

a) on the trusted list provider, the issuing scheme, i.e. the relevant scheme underlying the issuance and maintenance of the TL;

b) on the TSPs recognized by the scheme;

c) on the service(s) provided by these TSPs and the current status of the service(s);

d) on the status history of each service.

## 4.3 TSL/TL trust model

TSL and TL are signed electronic documents. To verify the signature, relying parties need to be able to access the applicable public key. Since the scheme under which the TSLs or TLs are issued is effectively positioned "above" the TSPs approved by that scheme, the authenticity of the public key cannot be verified solely on the basis of its certification by any TSP inside or outside the scheme. Providing the scheme's public key is therefore a problem very similar to providing the public key of a CA service.

NOTE: A possible solution to this problem is the publication of such public keys in the relevant Official Journals.

In the case where several TSLs or TLs participate to a common approval scheme or when there is a need to group and facilitate access to such TSLs or TLs, a compiled list of pointers towards such TSLs or TLs can be established, published and maintained.

Such a compiled list of pointers towards logically grouped TSLs or TLs can also play an important role in authenticating and trusting each TSL or TL which is pointed to by the compiled list. As a TSL or TL is signed by its provider, the certificate (or public key) to be used to verify such a signature can be included in the compiled list together with the corresponding pointer to this TL. The compiled list of pointers can be signed and the certificate to be used to verify the signature on the compiled list can be published in an official journal or in another trustworthy publication.

## 4.4 Providers of trust service status list or trusted lists

The TSL/TL providers (also called approval scheme operators) establishing, publishing and maintaining TLs or TSLs can be considered as a specific type of trust service provider and the issuance of TLs and TSLs considered a specific type of trust service.

The recognition and trustworthiness of such trust service providers is likely to depend on applicable legislation and/or on policy and security requirements on their practices and the policies they use to provide their services related to the establishing, publication and maintenance of their TLs or TSLs.

## 4.5 Aspects of TSL/TL provisioning services subject to standardization

Similarly to other types of TSPs described in clause 4.1, several aspects of TSL/TL are subject to standardization.

This covers:

a) **Policy & security requirements:** In order to ensure the trustworthiness of a TSL/TL provider it is important that the security and business practices of such TSP meet the recognized best practices for such services. Any weaknesses in the TSL/TL provider practices can potentially lead to significant risk of compromise to such TSP's services and so break the trust that the TSL/TL relying parties have in being able to ensure the security of its own transactions based on the TSL/TL they issue.

   Through standardization of such best practices, there is a recognized level of trust on which the TSL/TL user can base its decision to use the TSL/TL. These standards will be laid out in such a way that they can be referred to by TSL/TL providers to specify what the basis of their operations is.

   A TSL/TL provider is likely to make use of specific system components (e.g. cryptographic devices, computer systems) which need to be secure for the overall operation of their services to be secure.

b) **Technical specifications:** In the present context, this mainly refers to specifications aiming to establish a common template and a harmonized way for a TSL/TL provider to provide information about the status and status history of the trust services from Trust Service Providers (TSPs) regarding compliance with the relevant approval scheme underlying the TSL/TL. The TSL/TL as specific types of trust service tokens include the required information and are encoded in a way that is understood by the relying parties.

c) **Conformity assessment:** In order to gain assurance that a TSL/TL provider applies the best practices expected for it to be trustworthy, it 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 TSL/TL provider's policies and practices meet the requirement laid out in the applicable (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 TSL/TL provider 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.

d) **Testing technical conformity & interoperability:** With the aim of helping implementers and accelerating the development of tools for creating and issuing TSLs/TLs, test suites are necessary for supporting the organization of interoperability testing events where different TSL/TL related applications can check their actual interoperability. Additionally, test suites to check conformity of TSL/TL against the relevant technical specifications are also subject to standardization.

# 5 Guidance on the implementation of TSLs/TLs and selection of standards

## 5.1 Business requirements analysis

The process of selecting the appropriate standards and options is applied to the TSL/TL and TSL/TL provider area as follows.

Firstly, the analysis of the business requirements should be based on:

a) the impact the provision of information about the status and status history of the trust services from TSPs regarding compliance with the relevant provisions of the underlying approval scheme has on the targeted relying parties;

b) the specific business, legislative and geographical context in which the provision of such lists and information they contain applies;

c) potential mutual recognition being sought with trust services and trust service providers in the applicable domain.

## 5.2 Policy and security requirements analysis

Secondly the process regarding the analysis of the practices and policy requirements as well as the conduction of a risk analysis relating to the provision of TSLs/TLs will be addressed in the relevant policy requirements document as identified in clause 5.5.

## 5.3 Business scoping parameters

The selection of standards and their options for the provision of TSLs/TLs depends on the following business scoping parameters:

a) Business domain: In particular whether the list is aimed to be:

   1) a trusted list to be established, published and maintained by an EU Member State or EEA country to which Commission Decision 2009/767/EC [i.4] as amended by Commission Decision 2010/425/EU [i.7] and Commission Decision 2013/662/EU [i.8] applies; or

   2) a trusted list to be established, published and maintained by a non-EU country or an international organization seeking for potential mutual recognition and/or interoperability with European trusted lists; or

   3) any other type of trust service status list; and

b) Whether a formal recognition is required, e.g. through an independent audit, that a TSL/TL provider meets recognized criteria (called policy requirements in the standards for this area) for being trustworthy to meet the legal or commercial requirements of the user community.

NOTE: So far the applicable European legislation on trusted lists (i.e. Commission Decision 2009/767/EC [i.4] as amended by Commission Decision 2010/425/EU [i.7] and Commission Decision 2013/662/EU [i.8]) does not require trusted list providers (i.e. public or private bodies issuing and managing EU MS national trusted list) to undergo conformity assessments. Their formal recognition is limited to the requirement for EU MS to notify to the European Commission the body responsible for the establishment, maintenance and publication of the trusted list, the notification of the location of the trusted list and of the certificate(s) to be used to validate the trusted list signature; those notified elements being included in the LOTL signed by the European Commission.

## 5.4 Technical implementation and further selection of standards

Given the selection choices, the standards for the TSP providing TSL/TL should be used as indicated in table 1.

This will also help TSL/TL providers in:

a) defining rules for instantiation of TSLs or TLs (for EUMS or for non-EU countries or international organization); and

b) defining editing and usage rules of instantiated TSLs or TLs (for EUMS or for non-EU countries or international organization).

**Table 1: Summary of guidance on selection of standards**

| Topic | TL - EU MS | TL - non EU & International Organizations | (Other) TSSL's |
|---|---|---|---|
| Practices | No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 611 [i.10] | No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 611 [i.10] | No standard available |
| List content provisions | Commission Decision 2009/767/EC [i.4] as amended by Commission Decision 2010/425/EU [i.7] and Commission Decision 2013/662/EU [i.8] (based on ETSI TS 119 612 [i.3]) | Ad hoc rules for editing (based on ETSI TS 119 612 [i.3]) | Ad hoc rules for editing (can be based on below listed standards) |
| List format | ETSI TS 119 612 [i.3] | ETSI TS 119 612 [i.3] | ETSI TS 102 231 [i.9].<br>Possible future standard(s):<br>• ETSI TS 119 602 [i.11] |
| List usage | Commission Decision 2009/767/EC [i.4] as amended by Commission Decision 2010/425/EU [i.7] and Commission Decision 2013/662/EU [i.8]<br>No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 172 [i.12] | Ad hoc rules for usage.<br>No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 172 [i.12] | Ad hoc rules for usage<br>No standard available. |
| Conformity Assessment for List issuers | No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 603 [i.13]<br>• ETSI TS 119 613 [i.14] | No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 603 [i.13]<br>• ETSI TS 119 613 [i.14] | No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 603 [i.13] |
| Testing conformance & interoperability | No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 614 [i.15] | No standard available yet.<br>Possible future standard(s):<br>• ETSI TS 119 614 [i.15] | No standard available. |

LEGEND: The following documents are not available yet:

- ETSI TS 119 611 [i.10].
- ETSI TS 119 602 [i.11].
- ETSI TS 119 603 [i.13].
- ETSI TS 119 613 [i.14].

- ETSI TS 119 614 [i.15].
- ETSI TS 119 172 [i.12].

NOTE 1: ETSI TS 119 603 [i.13] and ETSI TS 119 613 [i.14] may only be considered necessary if there is a requirement for formal recognition through conformity assessment against the applicable criteria.

NOTE 2: Specific guidance and specifications for validating electronic signatures against EU Member States trusted lists is expected to be found in ETSI TS 119 172 [i.12] as part of the specifications regarding the corresponding signature validation policy.

NOTE 3: As a general guidance, TSL/TL providers need to consider standards in TSP supporting digital signatures and Trust Application Service Providers described in clause 4.1 and in particular the various classifications to distinguish categories or classes of TSPs and TASPs that would be approved and listed in the concerned TL or TSL.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | May 2015 | Publication |
| | | |
| | | |
| | | |
| | | |