ETSI TS 119 612 V1.2.1 (2014-04)

Electronic Signatures and Infrastructures (ESI);
Trusted Lists

Reference
RTS/ESI-0019612v121

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 Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

It is intended that the present document replaces TS 102 231 [i.6] to support the implementation of European Union Member State (MS) trusted lists as a means to express trust service status information with regards to their compliance with the relevant provisions laid down in Directive 1999/93/EC [i.3] and in related national laws.

Introduction

The purpose of the present document is to establish a common template and a harmonized way for a Trusted List Scheme Operator (TLSO) to 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 electronic signatures and trust services for electronic transactions.

NOTE 1: The terms "trust service" and "trust service provider", as defined in clause 3, include and are used with a broader application than the terms "certification service" and "certification service provider" used in Directive 1999/93/EC [i.3].

Trusted lists as established in EU by Commission Decision 2009/767/EC [i.2], aim primarily at supporting the validation of Qualified Electronic Signatures (QES) and Advanced Electronic Signatures (AdES) supported by a Qualified Certificate ($AdES_{QC}$) in the meaning of Directive 1999/93/EC [i.3] as far as they include at least trust service providers supervised/accredited for issuing qualified certificates. TLSOs can however include in their trusted lists also other types of approved trust service providers. Hence, electronic services based on AdES would also have their cross-border use facilitated, provided that the supporting trust services (e.g. issuing of non-qualified certificates) are part of the listed supervised/accredited services.

Trusted lists, as specified by the present document, 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 necessarily contain information from which it can be established whether the TSP's service is, or was, known by the Trusted List Scheme Operator (TLSO) 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, a receiving party would need 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.3]. 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 may also need to verify whether the signature is supported by a secure signature creation device.

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.

LOTL also plays an important role in authenticating EU MS trusted lists. Each national trusted list is electronically signed by its MS scheme operator and the certificate to be used to verify such a signature is included in the LOTL after notification to the European Commission. The authenticity and integrity of the machine processable version of the LOTL is ensured through a qualified electronic signature supported by a qualified certificate which can be authenticated and directly trusted through one of the digests published in the Official Journal of the European Union.

In the context of countries outside the European Union and the EEA countries, or in the context of international organizations, TLSOs may issue trusted lists in accordance with the present document. The benefits from the adoption of the present document by non-EU countries or international organizations are twofold:

- This may 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.
- 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 2: 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:

- provide information on the issuing scheme, i.e. the relevant scheme underlying the issuance and maintenance of the TL;
- identify the TSPs recognized by the scheme;
- indicate the service(s) provided by these TSPs and the current status of the service(s);
- indicate for each service the status history of that service.

1 Scope

The present document specifies a format and mechanisms for establishing, locating, accessing and authenticating a trusted list which makes available trust service status information so that interested parties may determine the status of a listed trust service at a given time. It defines the format and semantics of a TL as well as the mechanisms for accessing TLs. It also provides guidance for locating and authenticating TLs.

The present document applies to European Union Member State (EU MS) trusted lists as a means to express trust service status information with regards to their compliance with the relevant provisions laid down in Directive 1999/93/EC [i.3] and in related national laws.

In the context of non-EU countries or international organizations, scheme operators may issue trusted lists in accordance with the present document to facilitate mutual recognition of electronic signatures.

In addition, the present document defines requirements for relying parties to use TLs and the status information held within them.

2 References

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

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

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

2.1 Normative references

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

[1] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[2] ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms".

[3] ETSI TS 101 903: "Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)".

[4] Void.

[5] W3C Recommendation Second edition (2008): "XML Signature Syntax and Processing".

NOTE: There is a more recent W3C Recommendation of 11 April 2013 (http://www.w3.org/TR/xmldsig-core1/), XML Sig version 1.1, which also supports eliptic curves.

[6] ISO/IEC 10646: "Information technology -- Universal Coded Character Set (UCS)".

[7] IETF RFC 2368: "The mailto URL scheme".

[8] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

[9] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[10] IETF RFC 5322: "Internet Message Format".

[11] FIPS Publication 180-4 (2012): "Secure Hash Standard (SHS)".

[12] IETF RFC 5646: "Tags for Identifying Languages".

[13] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[14] ISO/IEC 6429: "Information technology - Control functions for coded character sets".

[15] ISO/IEC 2022: "Information technology - Character code structure and extension techniques".

[16] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".

[17] ISO 8601:2004: "Data elements and interchange formats - Information interchange - Representation of dates and times".

2.2 Informative references

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

[i.1] ETSI TS 102 853: "Electronic Signatures and Infrastructures (ESI); Signature validation procedures and policies".

[i.2] 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. OJ L 274, 20.10.2009, p. 36.

[i.3] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[i.4] W3C Recommendation of 11 April 2013: "XML Signature Syntax and Processing Version 1.1".

NOTE: Available at http://www.w3.org/TR/xmldsig-core1/. XML Sig version 1.1 also supports eliptic curves.

[i.5] ISO/IEC 9594-8:2005: "Information technology - Open System Interconnection - The Directory: Public-key and attribute certificate frameworks".

[i.6] ETSI TS 102 231 (V3.1.2): "Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information".

[i.7] W3C Technical Report #20 Revision 7: "Unicode in XML and other Markup Languages".

[i.8] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates".

[i.9] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile".

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.3], an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

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

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

approval: assertion that a trust service, falling within the oversight of a particular scheme, has been either positively endorsed or assessed for compliance against the relevant requirements (active approval) or has received no explicit restriction since the time at which the scheme was aware of the existence of the said service (passive approval)

approval scheme: any organized process of supervision, monitoring, assessment or such practices that are intended to apply oversight with the objective of ensuring adherence to specific criteria in order to maintain trust in the services under the scope of the scheme

Certification Authority (CA):

1) a trust service provider that creates and assigns public key certificates; or

2) a certificate generation trust service that is used by a trust service provider that creates and assigns public key certificates.

NOTE: See clause 4 of EN 319 411-2 [i.8] for further explanation of the concept of certification authority.

Certification Service Provider (CSP): entity or a legal or natural person who issues certificates or provides other services related to electronic signatures [i.3]

conformity assessment: process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled

Qualified Certificate (QC): public key certificate which meets the requirements laid down in Directive 1999/93/EC [i.3] annex I, and is provided by a certification service provider who fulfils the requirements laid down in its annex II

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

scheme operator: body responsible for the operation and/or management of any kind of assessment scheme, whether they are governmental, industry or private, etc.

Secure Signature Creation Device (SSCD): signature-creation device, as defined in Article 2.5 of [i.3], which meets the requirements laid down in annex III of [i.3]

signatory: person who creates an electronic signature

supervision system: system that allows for the supervision of trust service providers and the services they provide, for compliance with relevant requirements

NOTE: Directive 1999/93/EC [i.3] requires Member States to establish an appropriate system allowing the supervision of CSPs which are established on their territory and issue qualified certificates to the public, ensuring the supervision of compliance with the provisions laid down in the Directive.

Trust Service (TS): electronic service which enhances trust and confidence in electronic transactions (typically, but not necessarily, using cryptographic techniques or involving confidential material)

Trust Service Provider (TSP): body operating one or more (electronic) 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.3].

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

NOTE: Examples of binary trust service tokens are: certificates, CRLs, Time Stamp Tokens, OCSP responses. Physical tokens may be devices on which binary objects (tokens or credentials) are stored. Equally, a token may be the performance of an act and the generation of an electronic record, e.g. an insurance policy or share certificate.

Trusted List (TL): 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: In the context of EU MS, and as further specified by CD 2009/767/EC as amended [i.2], 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.3].

In the context of non-EU countries or international organizations, it refers to a list meeting the requirements of the present document 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.

Trust Service status List (TSL): form of a signed list as the basis for presentation of trust service status information

(voluntary) accreditation: any permission, setting out rights and obligations specific to the provision of trust services, to be granted upon request by the trust service provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the trust service provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body

NOTE: Based on Directive 1999/93/EC [i.3].

3.2 Abbreviations

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

ACA	Attribute Certification Authority
AdES	Advanced Electronic Signature
$AdES_{QC}$	Advanced Electronic Signature supported by a Qualified Certificate
AP	Asia Pacific
ARL	Authority Revocation List
BES	Basic Electronic Signature
BMP	Basic Multilingual Plane
CA	Certification Authority
CC	Country Code
CP	Certificate Policy
CPS	Certificate Practices Statement
CR	Carriage Return
CRL	Certificate Revocation List
CSP	Certification Service Provider
DN	Distinguished Name
EC	European Commission
ECDSA	Elliptic Curve Digital Signature Algorithm
EDS	Electronic Delivery Service
EEA	European Economic Area
EL	country code for Greece
EPES	Explicit Policy-based Electronic Signature
EU	European Union
EUMS	European Union Member States

FTP	File Transfer Protocol
GCC	Gulf Cooperation Council
GTC	General Terms & Conditions
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
LF	Line Feed
LOTL	List Of Trusted Lists
MS	Member State
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OJEU	Official Journal of the European Union
PIN	Personal Identification Number
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PSES	Preservation Service for Electronic Signatures
QC	Qualified Certificate
QES	Qualified Electronic Signature
RA	Registration Authority
REM	Registered Electronic Mail
RGS	Le Référentiel Général de Sécurité
RTF	Rich Text Format
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SSCD	Secure Signature Creation Device
TAB	Tabulator
TC	Technical Committee
TDP	TL Distribution Point
TL	Trusted List
TLSO	Trusted List Scheme Operator
TrST	Trust Service Token
TSA	Time Stamping Authority
TSL	Trust-service Status List
TSP	Trust Service Provider
TST	Time Stamp Token
UCS	Universal Character Set
UK	United Kingdom
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
UTF	Unicode Transformation Format
WWW	World Wide Web
XAdES	XML Advanced Electronic Signature
XHTML	eXtended HTML
XML	eXtensible Markup Language

4 Overall structure of Trusted Lists

Trusted List Scheme Operators (TLSO) which maintain a TL in compliance with the present document shall comply with:

- the format and semantics of a TL, as specified in clause 5;
- the mechanisms to be used to support relying parties locating, accessing and authenticating TLs, as specified in clause 6.

The logical model of the trusted list is shown in figure 1.

It has the following logical component parts. There shall be only one occurrence of the first two and last components (i.e. 1., 2. and 6.). The other components may be replicated as illustrated in figure 1:

1) A trusted list tag (**Tag)**: This tag facilitates the identification of the trusted list during electronic searches. The contents of the tag are specified in clause 5.2.1.

2) Information on the trusted list and its issuing scheme (**Scheme information**): The list commences with key information about the list itself and the nature of the scheme which has determined the information found in, and through, the list. This TL and scheme information is specified in clause 5.3 and it includes:

   - A trusted list format version identifier.
   - A trusted list sequence (or release) number.
   - A trusted list type information (e.g. for identification of the fact that this TL is providing information on the supervision/accreditation status of trust services from TSPs supervised/accredited by the referenced Member State for compliance with the provisions laid down in Directive 1999/93/EC [i.3]).
   - A trusted list scheme operator information (e.g. name, address, contact information of the body in charge of establishing, publishing securely and maintaining the trusted list).
   - Information about the underlying approval scheme(s) to which the trusted list is associated, including but not limited to:
     - the country in which it applies,
     - information on or reference to the location where information on the approval scheme(s) can be found (scheme model, rules, criteria, applicable community, type, etc.),
     - period of retention of (historical) information.
   - Trusted list policy and/or legal notice, liabilities, responsibilities.
   - Trusted list issue date and time and next planned update.

3) Unambiguous identification information about every TSP recognized in the scheme (**TSP information**): It is a sequence of fields holding unambiguous identification information about every listed TSP under the scheme. The contents of the TSP information fields are specified in clause 5.4 and include:

   - The TSP organization name as used in formal legal registrations.
   - The TSP address and contact information.
   - Additional information on the TSP either included directly or by reference to a location from where such information can be downloaded.

4) For each of the listed TSPs, the details of their specific trust services (**Service information**) whose current status is recorded within the TL are provided as a sequence of fields holding unambiguous identification of a listed trust service provided by the TSP. The contents of the service information field are specified in clause 5.5 and it includes the following for each trust service from a listed TSP:

   - An identifier of the type of service (e.g. identifier indicating that the listed trust service from the TSP is a certification authority issuing QCs).
   - (Trade) name of this service.
   - An unambiguous unique identifier of the service.
   - An identifier of the current status of the service.
   - The current status starting date and time.
   - Additional information on the service (directly included or included by reference to a location from which information can be downloaded): service definition information provided by the scheme operator, access information with regards to the service, service definition information provided by the TSP and service information extensions.

5) (**Service approval history**) For each listed trust service, information on the status history when applicable is available in the service approval history information or a sequence of such information. The contents of the history information fields are specified in clause 5.6.

6) (**Signature**) The TL is a signed list for authentication purposes. The contents of the signature field are specified in clause 5.7.

The number of TSPs, of services per TSP, and of history sections per service is unbounded.

The structure of the TL is further described in the following clauses by each component part and its fields.

In the context of a TSP issuing QCs, the structure of the trusted list and in particular the service information component (as per point 4 above) allows for complementary information in service information extensions to compensate for those situations where not enough information is available within the qualified certificate about its 'qualified' status, its potential support by an SSCD and especially in order to cope with the additional fact that most of the (commercial) TSPs are using one single issuing CA to issue several types of end-entity certificates, both qualified and non-qualified.

In the context of certificate generation (CA) services, the number of service entries in the list for a TSP may be reduced where one or several upper CA services exist within the TSP PKI (e.g. in the context of a hierarchy of CAs from a Root CA down to several issuing CAs) by listing such upper CA services and not the CA services issuing end-entity certificates (e.g. listing the TSP Root CA only). However in those cases, the status information applies to the whole hierarchy of CA services below the listed service.

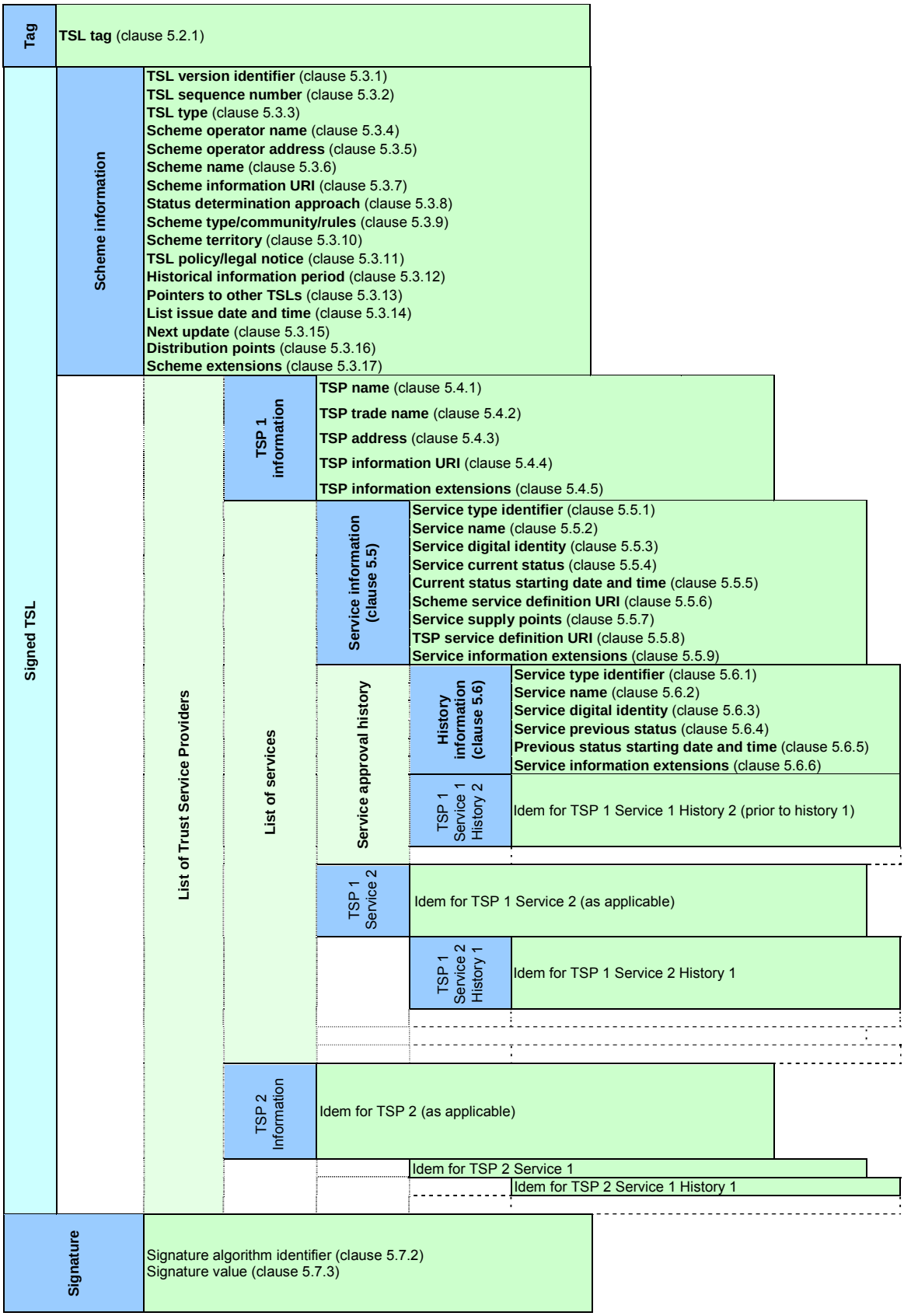

Figure 1: Logical model of the trusted list

5 Trusted list format and content

5.1 General principles for trusted lists

5.1.1 Trusted List Format

A TL shall be issued in XML format as specified in annexes B and C.

If the scheme operator or any party provides means to represent one TL in different formats, they shall contain exactly the same information as provided in the XML format of the TL.

5.1.2 Use of Uniform Resource Identifiers

In the definitions of TL fields given in the present document, many use uniform resource identifiers (URIs) to indicate the meaning of the field concerned. Within these definitions a "common name" may be used to broadly and simply describe the specific values or meanings of the field. These common names are linked to their declaration in annex D, which formally states all specific URIs used in the present document, with their meanings.

Some fields allow to use different URIs, which have the same purpose, to be registered and described by the scheme operator or another entity and recognized by the intended user community. Such URIs may be registered with ETSI. Information on URI registration can be found in clause D.3.

Where fields are defined as being of or using the type URI, implementers shall use general syntax as specified by RFC 3986 [9].

5.1.3 Date-time indication

All fields carrying date-time values shall comply with the following rules:

1) the date-time values shall be a character string formatted according to ISO 8601 [17]; and

2) the date-time value shall be expressed as Coordinated Universal Time (UTC): its value shall contain year with four digits, month, day, hour, minute, second (without decimal fraction) and the UTC designator "Z". The time scale shall be based on the second.

5.1.4 Language support

Trusted lists shall be issued supporting at least the UK English language, using the 'en' language code as specified in RFC 5646 [12] and annex E, and may be issued supporting multiple (national) languages.

For all the fields where support of multiple language is applicable, the field format specifications refer to the use of multilingual character string or pointer to which the following general rules shall apply:

1) A **multilingual character string** shall be a character string as defined in ISO/IEC 10646 [6] encoded in UTF-8. Each **multilingual character string** shall consist of two parts: a tag, conformant to RFC 5646 [12] and in lower case, that identifies the language in which the string is expressed, and the text in that language. The same content may be represented in multiple languages by a sequence of multilingual character strings.

2) A **multilingual pointer** shall be a URI that identifies a resource expressed in a particular language. Each **multilingual pointer** shall consist of two parts: a tag, conformant to RFC 5646 [12], that identifies the language in which the content pointed-to by the URI is expressed, and the URI expressed as a character string with the syntax specified by RFC 3986 [9], identifying a resource expressed in the given language. The same content may be represented in multiple languages by a sequence of multilingual pointers.

Whenever the native terms cannot be represented using the Latin alphabet, as defined in ISO/IEC 10646 [6], one issue of the term in the native language plus one issue with a transliteration to the Latin alphabet shall be used.

NOTE: Implementers should also comply with the UNICODE Standard (available at http://www.unicode.org/standard/standard.html).

Further detailed requirements regarding multilingual implementation are specified in normative annex E.

5.1.5 Value of Country Code fields

All fields carrying Country Codes values, denoted by "CC", shall be in capital letters and in accordance with either:

a) ISO 3166-1 [16] Alpha 2 codes with the following exceptions:

   1) the Country Code for United Kingdom shall be "UK";

   2) the Country Code for Greece shall be "EL";

   3) when the scope of the field is the European Union and/or the European Commission the code "EU" shall be used;

b) or commonly used extensions with regional scope (e.g. AP for Asia Pacific, ASIA);

c) or another identifier recognized for identifying multi-state grouping and that does not conflict with a), or b) (e.g. GCC, ASEAN).

5.2 Trusted List tag

5.2.1 TSL Tag

Presence: This field shall be present.

Description: The TL is tagged to facilitate its identification during electronic searches.

Format: A character string which indicates that the data structure is a TL. This shall be the character representation of the TSLTag URI.

Value: A unique value enabling a web-searching tool to establish during a WWW-wide search for TLs that a resource it has located is indeed a TL. Only the characters required to fully represent the URI shall be present.

5.3 Scheme information

5.3.1 TSL version identifier

Presence: This field shall be present.

Description: It specifies the version of the TL format.

Format: Integer.

Value: It shall be "**4**".

NOTE 1: This field will only be incremented when the rules for parsing the TL change, e.g. through addition/removal of a field or a change to the values or meaning of an existing field. Revisions to the specification which do not change the parsing rules of the TL may be made without revision to this field.

NOTE 2: The value of this field has been changed from "3" to "4" from TS 102 231 V3.1.2 [i.6] with regards to changes made to the values or meaning of existing fields (e.g. clauses 5.3.1, 5.3.3, 5.3.8, 5.3.9, 5.3.12, 5.5.1, 5.5.3, 5.5.4, 5.5.9.2.3, 5.7, 6) and some changes to the associated xml schema. Appropriate transition period where implementations consuming TL should support both set of specifications should be taken into account.

5.3.2 TSL sequence number

Presence: This field shall be present.

Description: It specifies the sequence number of the TL.

Format: Integer.

Value: At the first release of the TL, the value of the sequence number shall be 1. The value shall be incremented at each subsequent release of the TL and shall not, under any circumstance, be re-cycled to "1" or to any value lower than the one of the TL currently in force.

5.3.3 TSL type

Presence: This field shall be present.

Description: It specifies the type of the trusted list. It permits a parser to determine the form of any following field to expect according to the present document.

Format: An indicator expressed as a URI.

Value: In the context of EU Member State trusted lists, the URI shall be set to "http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric" as defined in clause D.5.

TLSOs from non-EU countries and international organizations shall use:

- the following URI as defined in clause D.6: "http://uri.etsi.org/TrstSvc/TrustedList/TSLType/CClist where "CC" (see clause 5.1.5) identifies the community to which the URI applies and is as used in the 'Scheme territory field' (clause 5.3.10); or
- a URI defined on purpose or registered under ETSI Identified Organization Domain as described in clause D.3 of the present document.

NOTE 1: In the context of EU Member States, it refers to a TL implementing a supervision/accreditation status list of trust services from trust service providers which are supervised/accredited by the referenced TLSO for compliance with the relevant provisions laid down in Directive 1999/93/EC [i.3] and through a process of direct oversight (whether voluntary or regulatory).

NOTE 2: In the context of non-EU countries or international organizations, it refers to a list meeting the requirements of the present document and providing assessment scheme based approval status information about trust services from trust service providers which are approved by the competent trusted list scheme operator or by the State or body in charge and from which the TLSO depends or by which it is mandated, for compliance with the relevant provisions of the applicable approval scheme and the applicable legislation. This may 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, 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). The adoption of the present document for such non-EU countries or international organizations trusted lists will facilitate the declaration of mutual recognition between trust services and trust services outputs.

When the TL contains exclusively a list of pointers towards other TLs and TL Issuers which are independently responsible for the approval or recognition of a community of trust services through a process of direct oversight (whether voluntary or regulatory), the URI shall be set to:

- "http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists" as defined in clause D.5 in the context of EU Member States' trusted lists; or
- in the context of non-EU countries and international organizations trusted lists, to:
  - "http://uri.etsi.org/TrstSvc/TrustedList/TSLType/CClistofthelists" as defined in clause D.6 where "CC" (see clause 5.1.5) identifies the community to which the URI applies and is as used in the 'Scheme territory field' (clause 5.3.10); or

- to a URI defined on purpose or registered under ETSI Identified Organization Domain as described in clause D.3 of the present document.

5.3.4 Scheme operator name

Presence: This field shall be present.

Description: It specifies the name of the entity in charge of establishing, publishing, signing and maintaining the trusted list.

Format: A sequence of multilingual character strings (see clause 5.1.4).

Value: The name of the scheme operator shall be the formal name under which the associated legal entity or mandated entity (e.g. for governmental administrative agencies) associated with the legal entity in charge of establishing, publishing and maintaining the trusted list operates. It shall be the name used in formal legal registration or authorization and to which any formal communication should be addressed.

5.3.5 Scheme operator address

Presence: This field shall be present.

Description: It specifies the address of the legal entity or mandated organization identified in the 'Scheme operator name' field (clause 5.3.4) for both postal and electronic communications.

Format: This is a multi-part field consisting of the scheme operator physical address specified in clause 5.3.5.1 Scheme operator postal address and the scheme operator electronic address specified in clause 5.3.5.2 Scheme operator electronic address.

5.3.5.1 Scheme operator postal address

Presence: This field shall be present.

Description: It specifies the postal address of the legal entity identified in clause 5.3.4, with the provision for the inclusion of the address in multiple languages.

Format: Sequence(s) of multilingual character strings (see clause 5.1.4).

Each sequence of character strings shall give the following attributes pertaining to the legal entity:

- street address (sub-components internally delimited by ";");
- locality (town/city);
- optionally, if applicable, State or Province name;
- postal code, if applicable;
- country name as a two-character code in accordance with clause 5.1.5 a).

Value: This shall be a postal address at which the scheme operator provides a help line service which is operated through conventional (physical) mail and which is processed as would be expected by normal business services.

Users (subscribers, relying parties) should use this address as the contact point for enquiries, complaints, etc. to the scheme operator.

5.3.5.2 Scheme operator electronic address

Presence: This field shall be present.

Description: It specifies both the email address and the web-site URI of the legal entity identified in clause 5.3.3 TSL type for electronic communications.

Format: A sequence of multilingual character strings (see clause 5.1.4) giving:

- e-mail address as a URI, in the form specified by RFC 3986 [9], with the URI scheme defined in RFC 2368 [7]; and
- web-site as a URI, in the form specified by RFC 3986 [9].

Both character strings shall be present.

Value: In the case of an e-mail address, this shall be an address at which the scheme operator provides a help line service which addresses TL-related matters and which is processed as would be expected by normal business services. In the case of a web-site URI, this shall lead to a capability whereby the user may communicate with a help line service which addresses TL-related matters and which is processed as would be expected by normal business services.

5.3.6 Scheme name

Presence: This field shall be present.

Description: It specifies the name under which the scheme operates.

Format: A sequence of multilingual character strings (see clause 5.1.4), defined as follows:

- The English version shall be a character string structured as follows:

  CC:EN_name_value

  where

  - 'CC' is the code used in the 'Scheme territory field' (clause 5.3.10);
  - ':' is used as the separator;
  - 'EN_name_value' is the name of the scheme.

- Any national language version shall be a character string structured as follows:

  CC:name_value

  where

  - 'CC' is the code used in the 'Scheme territory field' (clause 5.3.10);
  - ':' is used as the separator;
  - 'name_value' is the national language official translation of the above EN_name_value.

Value: The name of the scheme shall be the name which is used in formal references to the scheme in question, shall be unique and shall not be used by any other scheme operated by the same entity.

5.3.7 Scheme information URI

Presence: This field shall be present.

Description: It specifies the URI(s) where users (relying parties) can obtain scheme-specific information.

Format: A sequence of multilingual pointers (see clause 5.1.4).

Value: The referenced URI(s) shall provide a path to information describing appropriate information about the scheme, including:

- scope and context of the trusted list,
- general description and detailed information about underlying (approval) scheme,
- information about the process and procedures followed:
  - by the TLSO, or the body from which it depends or by which it is mandated, being in charge to approve TSPs, and
  - by the TSPs for being approved.
- information about the criteria against which TSPs are approved,
- information about the criteria and rules used to select assessors and defining how TSPs are assessed by them,
- where separate bodies provide separate aspects of supervision, accreditation and scheme operation, the separate responsibilities and any liabilities of each body, and
- other contact and general information that may apply to the scheme operation.

5.3.8 Status determination approach

Presence: This field shall be present.

Description: It specifies the identifier of the status determination approach.

Format: An indicator expressed as a URI.

Value: In the context of EU Member State trusted lists, the URI shall be set to "http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate" as defined in clause D.5.

TLSOs from non-EU countries and international organizations shall use either:

- the "http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/CCdetermination" URI as defined in clause D.6 and where "CC" is replaced by the code used in the 'Scheme territory field' (clause 5.3.10); or
- a URI defined on purpose or registered under ETSI Identified Organization Domain as described in clause D.3 of the present document.

5.3.9 Scheme type/community/rules

Presence: This field shall be present.

Description: It specifies the URI(s) where users (relying parties) can obtain scheme type/community/rules information against which services included in the list are approved and assessed, and from which the type of scheme or community may be determined.

Format: A sequence of multilingual pointers (see clause 5.1.4).

Value: The referenced URI(s) shall identify:

- the specific policy/rules against which services included in the list are approved and assessed, and from which the type of scheme or community may be determined;
- the description about how to use and interpret the content of the trusted list.

Where more than one URI is provided, each shall be a complete subset of the policy defined by its predecessor (e.g. a supra-national policy might be overarching; separate nations part of this supra-national entity may have their own implementations as part of this supra-national high-level policy).

When TLSOs participate to a wider scheme for issuing trusted lists which share common rules and which point towards a descriptive text that applies to the TL of each TLSO, a URI common to all TLSO shall be used:

- denoting participation of the trusted list (identified via the "TSL type" (see clause 5.3.3) and "Scheme name" (clause 5.3.6)) in a wider scheme of trusted lists (i.e. a TL listing pointers to all members publishing and maintaining a trusted list);
- identifying a resource from where users can obtain policy/rules against which services included in the lists are assessed;
- identifying a resource from where users can obtain description about how to use and interpret the content of the trusted lists. These usage rules shall be common to all trusted lists being part of the wider scheme of schemes whatever the type of listed services.

  In the context of EU Member States' trusted lists, this common URI shall be set to "http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon" as defined in clause D.5.

This field shall include a URI specific to a country's (national) trusted list and point towards a descriptive text that applies to this country's (national) TL:

- using the following URI as defined in clause D.4:

  http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC;

  where CC is replaced by the code used in the 'Scheme territory' field (clause 5.3.10);

  TLSOs may define additional URIs from the above specific URI (i.e. sub-URIs defined from this specific URI used as root). The definition and management of the sub-structure under the above URIs is under the responsibility of the TLSO;
- or, in the context of non-EU countries and international organizations only, using a URI defined on purpose or registered under ETSI Identified Organization Domain as described in clause D.3 of the present document.

5.3.10 Scheme territory

Presence: This field shall be present.

Description: It specifies the country or territory in which the scheme is established and applies.

Format: Character string in accordance with clause 5.1.5.

5.3.11 TSL policy/legal notice

Presence: This field shall be present.

Description: It specifies the scheme's policy or provides a notice concerning the legal status of the scheme or legal requirements met by the scheme for the jurisdiction in which the scheme is established and/or any constraints and conditions under which the TL is maintained and published.

Format: Either:

a) a sequence of multilingual pointers (see clause 5.1.4) for specific use as a pointer to the policy or notice; or

b) the actual text of any such policy or notice, as a multilingual character string (see clause 5.1.4).

Value: Any referenced text shall provide information describing the policy under which the Scheme Operator operates or any relevant legal notices with which users of the TL should be aware.

5.3.12 Historical information period

Presence: This field shall be present.

Description: It specifies the duration over which historical information in the TL is maintained once it has been included.

Format: Integer.

Value: The value of this integer shall be '65535', which signifies that historical information provided in the trusted list shall never be removed.

5.3.13 Pointers to other TSLs

Presence: This field shall be present for EU Member States' trusted lists. It is optional for non-EU countries and international organizations.

Description: It references any relevant trusted list or any relevant list of trusted lists.

Format: Sequence of one or more tuples, each tuple giving:

a) a string containing the URI of the machine processable format of another TL;

b) one or more digital identities, all representing the issuer of the TL pointed to, formatted as specified in clause 5.5.3; and

c) additional information as a set of TL Qualifiers: TSLType, as defined in clause 5.3.3; Scheme operator name, as defined in clause 5.3.4; Scheme type/community/rules, as defined in clause 5.3.9; Scheme territory, as defined in clause 5.3.10; and Mime type, as one of the media types defined in clause 6.1.1.2.1.

Value: More than one digital identity may be used to help the management of the pointed-to list signing process (e.g. in case of expiration/substitution of pointed-to list signing keys or more than a single signing key is allowed to sign this list). One of such digital identities shall allow successful authentication of the pointed-to list before its use.

In the context of EU Member State trusted lists, this field shall include the pointer to a European Commission compiled list of links (pointers) towards all trusted lists from the Member States, the so-called List Of Trusted Lists (LOTL) as it is notified in the Official Journal of the European Union. The referenced digital identities, validly representing the issuer(s) of the LOTL pointed to, formatted as specified in clause 5.5.3 shall be as published in the Official Journal of the European Union.

For non-EU countries and international organizations, this field may reference any relevant trusted list or list of trusted lists (e.g. the European List Of Trusted List as it is notified in the Official Journal of the European Union).

5.3.14 List issue date and time

Presence: This field shall be present.

Description: It specifies the date and time on which the trusted list was issued.

Format: Date-time value (see clause 5.1.3).

Value: Coordinated Universal Time (UTC) at which the TL was issued.

5.3.15 Next update

Presence: This field shall be present.

Description: It specifies the latest date and time by which the next planned update of the TL will be made available by the scheme operator or be null to indicate a closed TL.

Format: Date-time value (see clause 5.1.3).

Value: Coordinated Universal Time (UTC) by which an updated TL shall be issued. The schema operator may issue other TL before the next planned TL and Next Update shall always be the same or greater than the next update of the previous TL. If a scheme ceases operations or halts publication of its TL a final version shall be published with all services' status shown as "expired" (see Service current status) and this field set null.

In the event of no interim status changes to any TSP or service covered by the scheme, the TL shall be re-issued by the time of expiration of the last TL issued. TL with a Next update occurring in the past shall be discarded as expired as a measure to reduce the risk of a substitution by an attacker with an old TL.

The difference between the 'Next update' date and time and the 'List issue date and time' shall not exceed six (6) months.

Applications shall consider, in the event they implement some caching mechanism, that other TLs could be issued and published before the next planned update. See annex I for further information on application of trusted lists.

5.3.16 Distribution points

Presence: This field is optional.

Description: When used, it specifies locations where the current TL is published and where updates to the current TL can be found.

Format: Non-empty sequence of URIs.

Value: Dereferencing the given URI will always deliver the latest update of this TL.

If multiple distribution points are specified, they all shall provide identical copies of the current TL or its updated version.

5.3.17 Scheme extensions

Presence: This field shall not be present for EU Member States' trusted lists. It is optional for non-EU countries and international organizations.

Description: It provides specific scheme-related information and enhancements that do not require a change in the version identifier, which can be interpreted by all accessing parties according to the specific scheme's rules.

Format: Sequence of Scheme extensions whose format is left open. Each extension shall have an indication of its criticality.

Value: Each extension of the sequence shall be selected by the TLSO according to the information it wishes to convey within its TL. The meaning and value of each extension shall be defined by its source specifications being either the TLSOs own definition or any other extension definition produced by another entity, such as a community or federation of schemes, a standards body, etc. The criticality indication shall have the same semantics as with extensions in X.509-certificates [1]. A system using TLs shall reject the TL if it encounters a critical extension it does not recognize, while a non-critical extension may be ignored if it is not recognized.

5.3.18 List of Trust Service Providers

Presence: If no TSP is or was approved in the context of the trusted list scheme, this field shall not be present.

If one or more TSP services are or were approved under the TL scheme, this field shall be present.

Description: List of TSPs and their trust services approved in accordance with the trusted list scheme.

Format: Sequence of TSP information (see clause 5.4).

Value: It shall contain a sequence identifying each TSP providing one or more of those approved services, with details on the status and status history of each of the TSP's services.

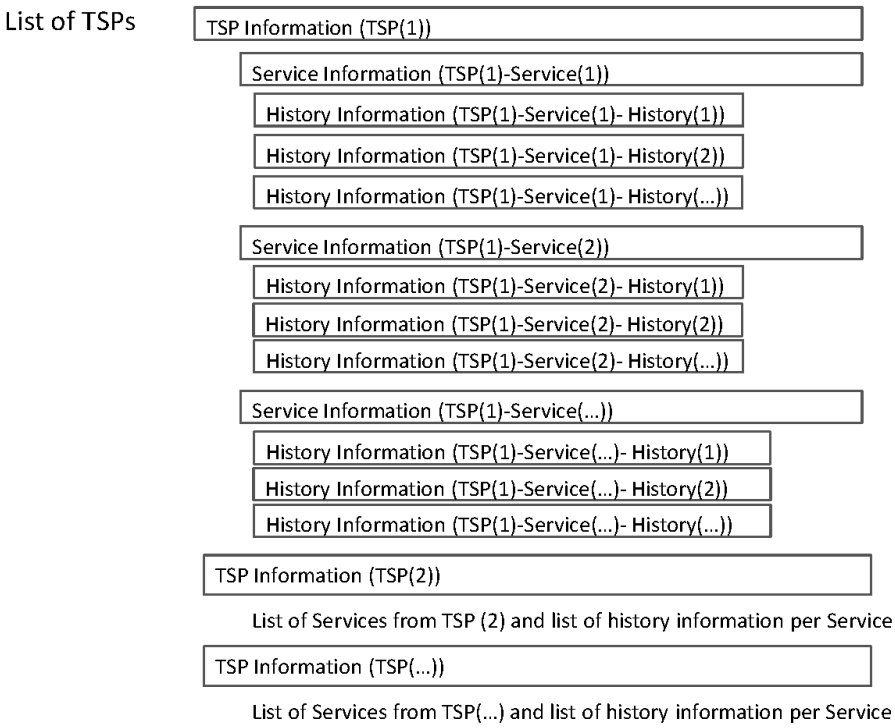

Figure 2

The list of TSPs shall be organized as depicted in figure 2. For each TSP, there is a sequence of fields holding information on the TSP (TSP Information), followed by a list of Services. For each of such listed Services, there is a sequence of fields holding information on the Service (Service Information), and a sequence of fields on the approval status history of the Service (Service approval history).

5.4 TSP information

5.4.1 TSP name

Presence: This field shall be present.

Description: It specifies the name of the legal entity, or when applicable the natural person, responsible for the TSP's services that are or were recognized by the scheme, in particular for the TSP's services that are or were approved under the applicable scheme.

Format: A sequence of multilingual character strings (see clause 5.1.4).

Value: The name of the legal entity, or when applicable the natural person, responsible for the TSP shall be the name which is used in formal legal registrations and official records and to which any formal communication, whether physical or electronic, should be addressed.

5.4.2 TSP trade name

Presence: This field shall be present.

Description: It specifies an official registration identifier as registered in official records, where such a registered identifier exists, that unambiguously identifies the TSP.

It may additionally be used to specify an alternative name under which the TSP identifies itself in the specific context of the provision of those of its services which are to be found in this TL under its 'TSP name' (clause 5.4.1) entry.

Format: A sequence of multilingual character strings (see clause 5.1.4).

Value: It shall include an official registered and unambiguous identifier and it may additionally include any name under which the legal entity, or when applicable the natural person, responsible for the TSP operates, in the specific context of the delivery of those of its services which are to be found in this TL.

NOTE: Where a single TSP legal entity, or when applicable a natural person, is providing services under different trade names or under different specific contexts, there might be as many TSP entries as such specific contexts (e.g. Name/Trade Name entries). An alternative is to list each and every TSP (legal entity or when applicable natural person) only once and provide Service specific context information. This is up to the Scheme Operator to discuss and agree with the TSP the most suitable approach.

5.4.3 TSP address

Presence: This field shall be present.

Description: It specifies the address of the legal entity or mandated organization, or when applicable the natural person, identified in the 'TSP name' field (clause 5.4.1) for both postal and electronic communications.

Format: This is a multi-part field consisting of the TSP physical address specified in clause 5.4.3.1 and the TSP electronic address specified in clause 5.4.3.2.

Value: In case of termination or cessation of the entire set of services provided by a listed TSP (e.g. bankruptcy), the TSP address shall be replaced by the address the Scheme Operator uses for enquiries about the terminated services (e.g. a specific dedicated email address and a specific webpage with relevant information including contact information).

5.4.3.1 TSP postal address

Presence: This field shall be present.

Description: It specifies the postal address of the TSP identified in clause 5.4.1, with the provision for the inclusion of the address in multiple languages.

Format: As specified in clause 5.3.5.1.

Value: This shall be a postal address at which the TSP provides a customer care or help line service, operated through conventional (physical) mail and processed as would be expected by normal business services.

5.4.3.2 TSP electronic address

Presence: This field shall be present.

Description: It specifies both the email address and web-site URI of the TSP identified in clause 5.4.1, to be used for electronic communications.

Format: As specified in clause 5.3.5.2.

Value: In the case of an e-mail address, this shall be an address at which the TSP provides a customer care or help line service which is related to the listed services and which is processed as would be expected by normal business services. In the case of a web-site URI, this shall lead to a capability whereby the user may communicate with a customer care or help line service which is related to the listed services and which is processed as would be expected by normal business services.

5.4.4 TSP information URI

Presence: This field shall be present.

Description: It specifies the URI(s) where users (e.g. relying parties) can obtain TSP-specific information.

Format: Sequence of multilingual pointers (see clause 5.1.4).

Value: The referenced URI(s) shall provide a path to information describing or leading to the description of the last and previous versions of the TSP's Practices Statements and/or Policies (e.g. CPS/CPs), the general terms and conditions of the TSP, legal issues, its customer care policies and other generic information which applies to all of its services listed under its TSP entry in the TL.

Where a single TSP entity is providing services under different trade names or under different specific contexts, and this has been reflected in as many TSP entries as such specific contexts, this field shall specify information related to the specific set of services listed under a particular TSP/TradeName entry.

In case of termination or cessation of the entire set of services provided by a listed TSP (e.g. bankruptcy), the TSP information URI shall be replaced by the specific URI the Scheme Operator uses for providing information about the terminated services (i.e. a specific dedicated webpage with relevant information) including the last and previous versions of the TSP's Practices Statements and/or Policies (e.g. CPS/CPs), GTC, maintained certificate validity status services or last CRL(s)/ARL(s) when all certificates have been revoked, etc.).

5.4.5 TSP information extensions

Presence: This field is optional.

Description: It may be used by scheme operators to provide specific TSP-related information, to be interpreted according to the specific scheme's rules.

Format: Sequence of TSP extensions whose format is left open.

Value: Each TSP information extension may be selected by the scheme operator according to the meaning and information it wishes to convey within its TL.

The meaning of each extension is hence defined by its source specification, that specification being either the scheme operator's own definition or any other extension definition produced by another entity, such as a community or federation of schemes, a standards body, etc.

In the context of EU Member State trusted lists, the TSP information extensions, when used, shall not be made critical.

5.4.6 List of services

Presence: This field shall be present.

Description: It contains a sequence identifying each of the TSP's recognized services and the approval status (and history of that status) of that service.

Format: Sequence of service information (see clause 5.5).

Value: At least one service shall be listed, even if the information held is entirely historical.

As the retention of historical information about listed services is required by clause 5.3.12, that historical information shall be retained even if the service's present status would not normally require it to be listed (e.g. the service is withdrawn). Thus a TSP shall be included even when its only listed service is in such a state, so as to preserve the history.

5.5 Service information

5.5.1 Service type identifier

Presence: This field shall be present.

Description: It specifies the identifier of the service type.

Format: An indicator expressed as a URI.

Value: The quoted URI shall be one of the following URIs, described in clause D.2, corresponding to the type of listed trust service or any other URI value registered and described by the scheme operator or another entity:

- certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services:

  http://uri.etsi.org/TrstSvc/Svctype/CA/QC

  When the listed service is a "root" certificate generation service issuing certificates to one or more sub-ordinates certificate generation services and from which a certification path can be established down to a certificate generation service issuing end-entity qualified certificates, this service type shall be further identified by using the "http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC" identifier (described in clause D.4) which is included in the additionalServiceInformation extension (clause 5.5.9.4) within a Service information extension (clause 5.5.9).

  TLSOs from non-EU countries or international organizations may use this URI to identify the type of listed trust services that are issuing certificates meeting equivalent requirements to those laid down in the European legislation and in this case should use the appropriate service information extension (see clause 5.5.9) to further identify those sets of certificates meeting such requirements, in particular the Qualification extension when applicable (see clause 5.5.9.2).

- certificate generation service creating and signing end-entity non-qualified certificates:

  http://uri.etsi.org/TrstSvc/Svctype/CA/PKC

- time-stamping generation service creating and signing time-stamp tokens:

  http://uri.etsi.org/TrstSvc/Svctype/TSA

- time-stamping generation service creating and signing qualified time-stamp tokens:

  http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST

NOTE 1: Such qualified time-stamp tokens are deemed to be issued in the context of the applicable legislation in the territory identified by the TL Scheme territory (see clause 5.3.10).

- time-stamping generation service, operated as part of services from a TSP issuing qualified certificates, creating and signing time-stamp tokens used to support QES and $AdES_{QC}$:

  http://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-QC

- time-stamping generation service creating and signing time-stamp tokens used to support QES and $AdES_{QC}$:

  http://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-AdESQCandQES

NOTE 2: This extension may be used whether or not the TSP providing such TSA services is issuing qualified certificates.

- certificate validity status services issuing Certificate Revocation Lists (CRLs):

  http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

- certificate validity status services issuing Certificate Revocation Lists (CRLs) and being part of a service from a TSP issuing qualified certificates:

  http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC

- certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses:

  http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

- certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and being part of a service from a TSP issuing qualified certificates:

  http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC

- registration services:

  http://uri.etsi.org/TrstSvc/Svctype/RA

- registration services that cannot be identified by a PKI-based public key:

  http://uri.etsi.org/TrstSvc/Svctype/RA/nothavingPKIid

- certificate generation service creating and signing attribute certificates:

  http://uri.etsi.org/TrstSvc/Svctype/ACA

- service responsible for issuing, publishing or maintenance of signature policies:

  http://uri.etsi.org/TrstSvc/Svctype/SignaturePolicyAuthorithy

- national root-CA services:

  http://uri.etsi.org/TrstSvc/Svctype/NationalRootCA-QC

- archival services:

  http://uri.etsi.org/TrstSvc/Svctype/Archiv

- registered electronic mail services:

  http://uri.etsi.org/TrstSvc/Svctype/REM

- electronic delivery services:

  http://uri.etsi.org/TrstSvc/Svctype/EDS

- electronic delivery services providing qualified electronic deliveries:

  http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

NOTE 3: Such qualified electronic deliveries are deemed to be issued in the context of the applicable legislation in the territory identified by the TL Scheme territory (see clause 5.3.10).

- preservation service for electronic signatures:

  http://uri.etsi.org/TrstSvc/Svctype/PSES

- preservation service for qualified electronic signatures:

  http://uri.etsi.org/TrstSvc/Svctype/PSES/Q

- Identity verification services:

  http://uri.etsi.org/TrstSvc/Svctype/IdV

- Key escrow services:

  http://uri.etsi.org/TrstSvc/Svctype/KEscrow

- Services issuing PIN- or password-based identity credentials:

  http://uri.etsi.org/TrstSvc/Svctype/PPwd

- Trusted list issuing services:

  http://uri.etsi.org/TrstSvc/Svctype/TLIssuer

- A trust service of an unspecified type:

  http://uri.etsi.org/TrstSvc/Svctype/unspecified

  When the "unspecified" Service type identifier is used, information about the nature and type of the listed service should be provided in other ways such as through a service level extension (see clauses 5.5.6 or 5.5.9).

  Non-EU countries and international organizations operating a scheme may create additional URIs for their own specific purposes or request ETSI to assign a URI root under the ETSI Identified Organization Domain, and then define its own URIs under this root, as described in clause D.3.

5.5.2 Service name

Presence: This field shall be present.

Description: It specifies the name under which the TSP identified in 'TSP name' (clause 5.4.1) provides the service whose type is identified in 'Service type identifier' (clause 5.5.1).

Format: A sequence of multilingual character strings (see clause 5.1.4).

Value: The name under which the TSP provides the service.

5.5.3 Service digital identity

Presence: This field shall be present.

Description: It specifies one and only one service digital identifier uniquely and unambiguously identifying the service.

Format: When not using PKI public-key technology (e.g. for a service with a service type identifier "http://uri.etsi.org/TrstSvc/Svctype/RA/nothavingPKIid"), an indicator expressed as a URI.

When using PKI public-key technology, a tuple giving:

- one or more X509Certificate elements expressed in Base64 encoded format as specified in XML-Signature [5];
- optionally, one X509SubjectName element that contains a Distinguished Name encoded as established by XML-Signature [5] in its clause 4.4.4;
- optionally, a public key value expressed as a ds:KeyValue element [5];
- optionally, a public key identifier expressed as an X.509 certificate Subject Key Identifier (X509SKI element) as specified in XML-Signature [5].

Value: When not using PKI public-key technology (e.g. for a service with a service type identifier "http://uri.etsi.org/TrstSvc/Svctype/RA/nothavingPKIid"), the indicator expressed as a URI shall be defined by the TLSO in a scheme specific context in such a way that it identifies uniquely and unambiguously the listed service.

When using PKI public-key technology, the service digital identifier uniquely and unambiguously identifying the service shall be a public key associated with the TSP service and used to verify the authenticity of the provided service.

EXAMPLE 1: The public key used for verifying signature on certificates, or the public key used for verifying signature on time-stamp tokens, or the public key for verifying signature on CRLs, or for verifying signature on OCSP responses, or more generally the public key used to verify signature on trust service outputs.

NOTE 1: This can be the public key of a CA issuing end-entity certificates (e.g. non qualified end-entity certificates in the case of a service of type "CA/PKC", or qualified certificates in case of a service of type "CA/QC") or the public key of a root CA belonging to the TSP and from which a path can be found down to end-entity qualified certificates issued under the responsibility of this TSP. Depending on whether or not this information and the information to be found in every end-entity certificate issued under this CA can be used to unambiguously determine the appropriate characteristics of any qualified certificate, this information (Service digital identity) may need to be completed by 'Service information extensions' data (see clause 5.5.9).

The service digital identifier shall be specified by at least one representation of this digital identifier. To represent this public key, implementations:

- shall use at least one X509Certificate element [5] representing the same public key. It should be represented by exactly one certificate. The TLSO may list more than one certificate to represent the public key, but only when all those certificates relate to the same public key and have identical subject names identifying the TSP identified in clause 5.4.1 as holder of the key. When candidate certificates for representing the same public key do not have subject names identical to subject names of certificates already representing the same key, the TLSO shall not use these certificates as representation of this service digital identifier.
- should additionally use the following representation of the same public key:
  - the X509SubjectName element [5] to which the public key relates under the form of a Distinguished Name;

This representation of the public key should not be used by applications in machine processable way.

- may additionally use one or both of the following representations of the same public key:
  - the public key value itself, i.e. a ds:KeyValue element [5];
  - the related public key identifier, i.e. the X.509 Certificate Subject Key Identifier (X509SKI element [5]).

  If public key representations are present more than once, all variants shall refer to the same public key.

  The same public key (and hence the same certificate representing this public key) shall not appear more than once in the trusted list for the same type of service. The same public key may appear more than once in the TL only when associated to trust services having different 'Service type identifier' ('Sti') values (e.g. public key used for verifying signatures on different types of Trust Services Tokens) for which different supervision/accreditation systems apply.

EXAMPLE 2: When a TSP is using the same private key to sign on the one hand QCs under an appropriate supervision system for qualified trust services and on the other hand to sign non-qualified certificates falling under a different supervision/accreditation system, then in this case, two entries with different 'Sti' values (e.g. respectively CA/QC and CA/PKC in the given example) and with the same public key as service digital identity would be used.

NOTE 2: Providing two or more certificates with the same public key is not regarded as two separate identifiers, but two representations of the same identifier provided they both have identical X.509 Subject Name values.

NOTE 3: The re-keying of a trust service is resulting in using a new service entry in the trusted list (one service entry per new public key).

When additional information needs to be provided with regard to the identified service entry, then, when appropriate, the TLSO shall consider the use of the 'additionalServiceInformation' extension (clause 5.5.9.4) of the 'Service information extension' field (clause 5.5.9) according to the purpose of providing such additional information. Additionally, the Scheme operator can optionally use the 'Scheme service definition URI' field (see clause 5.5.6).

NOTE 4: The same public key (and hence private key) are not expected to be allocated to different subject names even if those names identify the same entity.

With regards to X.509 Certificates that are candidates to represent a public key identifying a listed service, the TLSO shall disregard certificates for which the "O=" attribute does not include the 'TSP Name' value (clause 5.4.1) **except** if no candidate certificate can be found to meet such a requirement. If the TSP cannot replace the candidate certificates for which the "O=" attribute fails to include the 'TSP Name' value (clause 5.4.1), the TLSO may include them in the TL. When doing so, the TLSO shall provide, for such listed certificates, a formal statement in the 'Scheme service definition URI' (clause 5.5.6) indicating that they are issued to and owned by the TSP identified by the 'TSP Name' value even if the 'TSP Name' value in the TL and the "O=" value in the certificate differ. Those "O=" values distinct from the 'TSP Name' value shall then be listed as 'TSP Trade Name' values (clause 5.4.2).

The content of the X509SKI element shall be the same as the content of the SubjectKeyIdentifier extension of the listed certificate(s).

TLSO and/or the body in charge to which it depends or by which it is mandated may decide to use the public key of a Root or Upper level CA **from this TSP** as the 'Sdi' of a single entry in the list of services from a listed TSP. The consequences (advantages and disadvantages) of such a decision shall be notified by the TLSO to the corresponding TSP. In addition, TLSOs shall provide in 'Scheme service definition URI' (clause 5.5.6) the necessary documentation to facilitate the certification path building and verification.

EXAMPLE 3: An example of use of the public key of a Root or Upper level CA is a Certification Authority not directly issuing end-entity QCs but certifying a hierarchy of CAs down to CAs issuing QCs to end-entities.

NOTE 5: Using a RootCA public key as 'Sdi' value for a listed service will force the TLSO to consider the whole set of trust services under such a Root CA as a whole with regards to its 'service status' (clause 5.5.4). The revocation being required for one single CA under the listed root hierarchy, will force the whole hierarchy to take-on that status change.

NOTE 6: When "Service digital identifiers" are to be used as Trust Anchors in the context of validating electronic signatures for which signer's certificate is to be validated against TL information, only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are considered as Trust Anchor certificates conveying identical information with regards to the information strictly required as Trust Anchor information.

5.5.4 Service current status

Presence: This field shall be present.

Description: It specifies the identifier of the current status of the service.

Format: An identifier expressed as an URI.

Value: In the context of EU Member States,

- to the exception of the "NationalRootCA-QC" service type, the identifier of the status of all the services shall be one of the following URIs as defined in clause D.5:
  - Under Supervision:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision"
  - Supervision of Service in Cessation:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation"
  - Supervision Ceased:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased"
  - Supervision Revoked:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionrevoked"
  - Accredited:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited"
  - Accreditation Ceased:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationceased"
  - Accreditation Revoked:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationrevoked"

  The TLSOs shall follow the "supervision/accreditation status flow" as depicted in clause D.5 for the use of the above listed 'Service current status' values for all types of listed trust services.

  When used in the context of a trust service provider issuing QCs that is established in the 'Scheme territory' (clause 5.3.10), the statuses 'Accreditation Revoked' and 'Accreditation Ceased' shall be considered as 'transit statuses'. They shall not be used as value for 'Service current status', but used as 'Service previous status' value immediately followed in the 'Service approval history information' or in the 'Service current status' by an 'Under supervision' status, potentially followed by any other supervision status listed here above and as illustrated in clause D.5.

The 'Accreditation Revoked' and 'Accreditation Ceased' statuses may be used as a value for 'Service current status':

- when used in the context of a trust service provider not issuing QCs and when there is only an associated 'voluntary accreditation' system with no associated supervision system; or
- in the context of a trust service provider issuing QCs where the trust service provider is not established in the 'Scheme territory' (clause 5.3.10).

When additional status-related 'qualification' information defined at the level of national supervision/accreditation systems for trust service providers not issuing QCs is available at service level (e.g. to distinguish between several quality/security levels), TLSOs shall use the 'additionalServiceInformation' extension (clause 5.5.9.4) of the 'Service information extension' field (clause 5.5.9) according to the purpose of providing such additional 'qualification' information. Additionally, TLSOs may use 'Scheme service definition URI' (clause 5.5.6).

- with regards to the "NationalRootCA-QC" service type (as defined in clause 5.5.1), the identifier of the status of such services shall be one of the following URIs as defined in clause D.5:
  - Set by national law:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/setbynationallaw"
  - Deprecated by national law:

    "http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedbynationallaw"

  The TLSOs shall follow the following status flow for the use of the above listed 'Service current status' values for listed trust services of type "NationalRootCA-QC":

  Start → "setbynationallaw" → "deprecatedbynationallaw" (end).

In the context of non-EU countries and international organizations the current status value shall be one of the values specified by the TLSO through the 'Scheme information URI' (see clause 5.3.7).

5.5.5 Current status starting date and time

Presence: This field shall be present.

Description: It specifies the date and time on which the current approval status became effective.

Format: Date-time value (see clause 5.1.3).

Value: Coordinated Universal Time (UTC) at which the current approval status became effective.

NOTE: The relying parties could apply this information by comparing it with other available information, e.g. the date and time on which a certificate or a time stamp was issued. From the comparison, the user could determine whether the specific service of the TSP had the desired approval status under the scheme at the date and time of provision of the service.

5.5.6 Scheme service definition URI

Presence: This field is optional.

Description: It specifies the URI(s) where relying parties can obtain service-specific information provided by the TL scheme operator.

Format: A sequence of multilingual pointers (see clause 5.1.4).

Value: The referenced URI(s) shall provide a path to information describing the service as specified by the scheme. In particular this may include:

a) URI indicating the identity of the fallback TSP in the event of the supervision of a service in cessation for which a fallback TSP is involved (see 'Service current status' - clause 5.5.4);

b) URI leading to documents providing additional information related to the use of some nationally defined specific qualification for an approved trust service token provisioning trust service in consistence with the use of 'Service information extension' field (clause 5.5.9) with an 'additionalServiceInformation' extension as defined in clause 5.5.9.4.

5.5.7 Service supply points

Presence: This field is optional.

Description: It specifies one or more URIs where relying parties can access the service.

Format: Non-empty sequence of URIs.

Value: The referenced URI(s) shall specify where and how the service can be accessed.

5.5.8 TSP service definition URI

Presence: When the service type (clause 5.5.1) is "NationalRootCA-QC", this field shall be present. In other cases, this field is optional.

Description: It specifies the URI(s) where relying parties can obtain service-specific information provided by the TSP.

Format: A sequence of multilingual pointers (see clause 5.1.4).

Value: The referenced URI(s) shall provide a path to information describing the service as specified by the TSP.

When the service type (clause 5.5.1) is "NationalRootCA-QC", this field shall specify the URI(s) where relying parties can obtain service-specific information provided by the TSP including details on the establishment and management rules of such services and relevant national legislation where rules for national root scheme exist in legislation.

5.5.9 Service information extensions

Presence: This field is optional.

Description: It specifies specific service-related information.

Format: Sequence of service information extensions, each of which is formatted as specified in next clauses and each of which may be selected by the TLSO according to the meaning and information it wishes or needs to convey within its TL.

Value: Pre-defined extensions are specified in next clauses with regards to:

- indication of the time from which a listed trust service creating and signing CRLs or signed OCSP responses keeps revocation notices for revoked certificates also after they have expired (see clause 5.5.9.1);
- information provided on characteristics of qualified certificates (i.e. qualified status, issuance to legal person, corresponding private key residing or not in an SSCD) created and signed by a listed trust service when such information is not part of the certificates (see clause 5.5.9.2);

- information on the taking over of a listed trust service by another trust service provider than the one identified by the TSP Name (clause 5.4.1), including the identification of the taking over trust service provider, the taking over process and its consequences on subscribers and relying parties (see clause 5.5.9.3);
- additional service information (see clause 5.5.9.4).

5.5.9.1 expiredCertsRevocationInfo Extension

Presence: This field is optional but may only be present when used with the following 'Service types' (clause 5.5.1):

- "CA/PKC";
- "CA/QC";
- "NationalRootCA-QC";
- "Certstatus/OCSP"; "Certstatus/OCSP/QC";
- "Certstatus/CRL"; "Certstatus/CRL/QC";
- other applicable service types defined by the TLSO in accordance to D3.

It shall not be used with other types.

This extension shall not be set critical.

Description: This extension supports the same function as in ISO/IEC 9594-8:2005 [i.5], clause 8.5.2.12.

It indicates:

- that the scope of each CRL and OCSP response, issued by the service to which this extension applies, is extended to include the revocation status of certificates that expired at the exact time specified in the extension or after that time;
- that the revocation status of a certificate will not be updated once the certificate has expired (this behaviour being openly allowed by ISO/IEC 9594-8:2005 [i.5] and RFC 5280 [13]); and
- that if limitations in the CRL's scope are specified (by either reason codes or by distribution points), they apply to expired certificates as well.

Format: Date-time value (see clause 5.1.3).

Value: If a CRL contains the extension expiredCertsOnCRL defined in [i.5] it shall prevail over the TL extension value but only for that specific CRL.

5.5.9.2 Qualifications Extension

Presence: This field shall be present when the information present in the qualified certificates created and signed by or under a listed trust service of the type "CA/QC" does not allow machine-processable identification

- of the fact that it is a claimed qualified certificate, and/or
- whether or not the private key corresponding to the certified public key resides in an SSCD, and/or
- whether the certificate has been issued to a legal person.

If this extension is marked "critical" a certificate validation process shall discard the certificate under validation if it cannot parse and understand its entire semantic.

Description: The qualifications extension is specified by a set of Qualification Elements, each one expressed as a list of assertions to be verified and a list of qualifiers that apply to the examined certificate when all the assertions are verified. The certificate is qualified with all the qualifiers obtained with the application of all the qualification elements.

Format: A non-empty sequence of one or more Qualification Elements defined below in clause 5.5.9.2.1. For the formal definition see `Qualifications` element in the schema referenced by clause C.2 (point 2).

5.5.9.2.1 QualificationElement

Presence: This field shall be present.

Description: This field bundles a list of assertions (criteria) that specifies the attributes identifying the certificates (e.g. certain key-usage-bits set) to which a list of qualifiers apply that specify some certificate properties (e.g. it is a qualified certificate, the corresponding private key resides in an SSCD or not, the subject of the certificate is a legal person).

Format: A tuple consisting of a list of assertions (CriteriaList, see clause 5.5.9.2.2) and a list of qualifiers (Qualifiers, see clause 5.5.9.2.3). For the formal definition see `QualificationElementType` element in the schema referenced by clause C.2 (point 2).

5.5.9.2.2 CriteriaList

Presence: This field shall be present.

Description: It provides a list of assertions related to certificate contents (e.g. key usage) and/or status (e.g. additional assessment) used to filter certificates. An assertion can be itself a CriteriaList allowing a recursive definition. An optional Description field allows the schema operator to specify the rationale of the defined criteria.

Format: A non-empty sequence of assertions whose syntax is specified in clauses 5.5.9.2.2.1 to 5.5.9.2.2.3 followed by a matching criteria indicator that can have the following values:

- "all" if all of the assertion shall be met;
- "atLeastOne" if at least one of the assertion shall be met; or
- "none" if all the assertions shall not be met;

for the given set of qualifiers, related to the CriteriaList, to apply.

For the formal definition see CriteriaListType element in the schema referenced by clause C.2 (point 2).

An optional Description field expressed as a character string. If present the description shall be expressed in UK English.

5.5.9.2.2.1 KeyUsage

Presence: This field is optional.

Description: It provides a list of key usage bit-values to match with the correspondent bits present in the keyUsage certificate Extension. The assertion is verified if the KeyUsage Extension is present in the certificate and all key usage bits provided are matched with the corresponding bit in the certificate KeyUsage Extension.

Format: A non-empty sequence of tuples composed by a Key Usage Bit identifier and the asserted value. The key usage bits identifiers shall be those defined in X.509 [1] for the KeyUsage Extension. For the formal definition see `KeyUsageType` element in the schema referenced by clause C.2 (point 2).

5.5.9.2.2.2 PolicySet

Presence: This field is optional.

Description: It provides list of Certificate Policy identifiers to match with the content of the CertificatePolicy certificate Extension. The assertion is verified if the CertificatePolicy Extension is present in the certificate and all the Certificate Policy identifiers provided are present in the certificate CertificatePolicy Extension.

Format: A sequence of one of more Object Identifiers indicating a Certificate Policy. For the formal definition see `PoliciesListType` element in the schema referenced by clause C.2 point 2).

5.5.9.2.2.3 OtherCriteria

Presence: This field is optional.

Description: It allows the inclusion of new criteria that can be required by TL Scheme Operators for additional assertions on certificate content/status. Here follows some OtherCriteria definition, new criteria can be added in future. If not included in the following list it is the responsibility of the TLSO that defines a new criteria to publish the related definition in an effective way.

1) ExtendedKeyUsage

Presence: This field is optional.

Description: It provides a non empty list of key purposes values to match with the correspondent KeyPurposes present in the ExtendedKeyUsage certificate Extension. The assertion is verified if the ExtendedKeyUsage Extension is present in the certificate and all key purposes provided are present in the certificate ExtendedKeyUsage Extension.

Format: A non-empty sequence of KeyPurposes, whose semantic shall be as defined in X.509 [1] for the ExtendedKeyUsage Extension. For the formal definition see `ExtendedKeyUsage` element in the schema referenced by clause C.2 (point 3).

2) CertSubjectDNAttribute

Presence: This field is optional.

Description: It provides a non empty set of OIDs. Each OID maps to a possible attribute in the Subject DN of the certificate. The criterion is matched if all OID refers to an attribute present in the DN.

Format: A non-empty sequence of OIDs representing Directory attributes, whose meaning respect the description above. For the formal definition see `CertSubjectDNAttribute` element in the schema referenced by clause C.2 (point 3).

5.5.9.2.3 Qualifier

Presence: This field shall be present.

Description: It specifies the properties a certificate with the specified criteria possesses.

Format: Sequence of indicators expressed as URIs.

Value: The following qualifiers shall only be used when the type of the service to which it applies is "CA/QC". They are defined in clause D5:

- **QCWithSSCD** ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD"): to indicate that all certificates identified by the applicable list of criteria, when they are claimed as being qualified, have their private key residing in an SSCD;
- **QCNoSSCD** ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD"): to indicate that all certificates identified by the applicable list of criteria, when they are claimed as being qualified, do not have their private key residing in an SSCD;

- **QCSSCDStatusAsInCert** ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCSSCDStatusAsInCert"): to indicate that all certificates identified by the applicable list of criteria, when they are claimed as being qualified, do contain proper machine processable information about whether or not their private key residing in an SSCD;
- **QCForLegalPerson** ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForLegalPerson"): to indicate that all certificates identified by the applicable list of criteria, when they are claimed as being qualified, are issued to legal persons;
- **QCStatement** ("http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement"): to indicate that all certificates identified by the applicable list of criteria are issued as qualified certificates.

  The QCStatement qualifier shall be used **with extreme caution** by MS Scheme Operators and Supervisory/Accreditation Bodies when and **only when**:

  - strong evidence exists that certificates identified through the applied filters are indeed to be considered as qualified certificates; **and**
  - no machine processable information is present in the certificates to indicate that it is used as a qualified certificate (i.e. no use of QcCompliance statement [i.9] or a QCP/QCP+ OID [i.8]).

5.5.9.3 TakenOverBy Extension

Presence: This field shall be present when a service that was formerly under the legal responsibility of a TSP is taken over by another TSP.

Description: It specifies the identity of the TSP having taken over the responsibility of the service to which this extension applies and is meant to state formally the nature of this legal responsibility and to enable the verification software to display to the user some legal detail.

Format: This extension contains an URI, and a sequence of the following attributes:

- The TSP name, as defined in clause 5.4.1.
- The Scheme operator name as specified in clause 5.3.4.
- The Scheme territory as specified in clause 5.3.10.
- An optional additional information field for further qualification of the taking over TSP, to be defined in future versions of the present document or by schema operators as schema specific.

Value: When a listed service is taken over by another TSP than the one under which the service is listed, the related service entry in the TL shall not be copied by the TLSO or moved inside the taking over TSP list of services and it is under the responsibility of the TLSO to maintain up to date the correct service trust state. If the taking over TSP issues a new digital identity related to the taken over service (e.g. a new self signed certificate for a CA) then a new service entry shall be created under the taking over TSP. If the previous service is still in operation, even for a limited scope (e.g. CRL issuing as for the example above) its status shall be maintained by the TLSO, according to the established rules, until the service terminates its operations.

This extension contains an URI, pointing towards a descriptive text that shall provide detailed information to the user about who is the entity currently responsible for the service and detailed information about the taken over process and its consequences on subscribers and relying parties.

In addition this extension contains a set of attributes, uniquely identifying the taking over TSP allowing the application to locate this TSP in the TL, if present, and to display its details.

The content of this extension is not meant to enforce any specific action on the signature validation.

If this extension is marked "critical" a certificate validation process shall discard the certificate under validation if it cannot parse and understand its entire semantic.

This extension shall be implemented with the `TakenOverBy` element defined in the schema referenced by clause C.2 (point 3).

5.5.9.4 additionalServiceInformation Extension

Presence: This field is optional.

Description: It specifies additional information on a service.

Format: A sequence of one or more tuples, each tuple providing the information detailed below. A TL may have more than one additionalServiceInformation extension in the same service entry, each extension giving:

a) an URI identifying the additional information. Possible values, not limited to the following:

- a registered URI to further qualify a "Service type identifier" (clause 5.5.1), in order to further specify the "Service type identifier" identified service as being a component service of a trust service provider issuing QC (e.g. "RootCA-QC" service type qualification extension of a "CA/QC" service type as specified in clause D.4);
- an URI indicating some nationally defined specific qualification for a supervised/accredited Trust Service Token provisioning service.

EXAMPLE:

- a specific security/quality granularity level with regard to national supervision/accreditation system for TSPs not issuing QCs (e.g. RGS */**/*** in France, specific "supervision" status set by national legislation for specific TSPs issuing QCs in Germany), see note 5 of "Service current status" - clause 5.5.4; or
- a specific legal status for a supervised/accredited Trust Service Token provisioning (e.g. nationally defined "qualified TST" as in Germany, Hungary or Italy); or
- meaning of a specific Policy identifier present in a X.509v3 certificate provided in "Sdi" field.

b) an optional string containing the serviceInformation classification, with a meaning as specified in the scheme (e.g. in France services are classified with specifically registered URI in line with the possible RGS classification values);

c) any optional additional information provided in a scheme-specific format.

Value: This extension may be used to provide, for a given service, additional information that may help to verify the applicability of the given service for a certain purpose.

Dereferencing the URI should lead to human readable information (as a minimum in UK English language and potentially in one or more national languages) which is deemed appropriate and sufficient for a relying party to understand the extension, and in particular explaining the meaning of the given URIs, specifying the possible values for serviceInformation and the meaning for each value.

5.5.10 Service approval history

Presence: This field shall be present only when historical information is applicable to the related service. In the case the service has no history prior to the current status (i.e. a first recorded status or history information not retained by the scheme operator) this field shall not be present.

Description: It specifies historical information on listed trust services as a sequence of all previous status entries which the scheme has recorded for the given TSP service.

Format: Sequence of History information (see clause 5.6).

Value: For each change in TSP service approval status which occurred within the historical information period as specified in clause 5.3.12, information on the previous approval status shall be provided in descending order of status change date and time (i.e. the date and time on which the subsequent approval status became effective).

5.6 Service approval history information

5.6.1 Service type identifier

Presence: This field shall be present.

Description: It specifies the identifier of the service type, with the Format and Value used in clause 5.5.1.

5.6.2 Service name

Presence: This field shall be present.

Description: It specifies the name under which the TSP provided the service identified in clause 5.5.1, with the Format and Value used in clause 5.5.2.

NOTE: This clause does not require the name to be the same as that specified in clause 5.5.2. A change of name may be one of the circumstances requiring a new status.

5.6.3 Service digital identity

Presence: This field shall be present.

Description: It specifies at least one representation of a digital identifier of the service used in clause 5.5.1, with the Format and Value used in clause 5.5.3.

5.6.4 Service previous status

Presence: This field shall be present.

Description: It specifies the identifier of the previous status of the service, with the Format and Value used in clause 5.5.4.

5.6.5 Previous status starting date and time

Presence: This field shall be present.

Description: It specifies the date and time on which the previous status in question became effective, with the Format and Value used in clause 5.5.5.

5.6.6 Service information extensions

Presence: This field is optional.

Description: It may be used by TLSOs to provide specific service-related information, to be interpreted according to the specific scheme's rules, with the Format and Value used in clause 5.5.9.

5.7 Signature

5.7.1 Signed Trusted List

The trusted list shall be signed by the 'Scheme operator name' (clause 5.3.4) to ensure its authenticity and integrity.

The format of the signature shall be XAdES BES or EPES as defined by TS 101 903 [3]. Such electronic signature implementation shall meet requirements as stated in annex B. The signature algorithm as well as the certified signature key shall conform to security requirement for a minimum 3 years usable key as specified in table 14 of TS 102 176-1 [2].

The TLSO certificate, to be used to verify its signature on the TL, shall be protected with the signature in one of the ways specified by TS 101 903 [3]. The SigningCertificate signed attribute (or property) available in TS 101 903 [3] signatures should be used for this purpose. The ds:keyInfo shall not contain any associated certificate chain.

The Scheme Operator signing certificate shall be conformant to the following restrictions:

- The Issuer shall be the TLSO itself (i.e. a self-signed certificate) or a TSP trust service listed in the TL or in one of the TL that is part of the same community (see clause 5.3.9).
- "Country code" and "Organization" fields in Subject Distinguished Name shall match respectively the "Scheme Territory" and one of the "Scheme operator name" values. For the latter, the value in UK English language (preferred) or local language (transliterated to Latin script), as available, should be used.
- KeyUsage extension shall be set only and exclusively to digitalSignature or nonRepudiation (contentCommitment).
- ExtendedKeyUsage extension should be present containing id-tsl-kp-tslSigning (see below).
- The use of the KeyUsage and ExtendedKeyUsage extensions shall be consistent with the purpose of signing trusted lists.
- SubjectKeyIdentifier extension shall be present using one of the first 2 methods specified in clause 4.2.1.2 of RFC 5280 [13].
- BasicConstraints extension shall indicate CA=false.

In order to indicate that the use of key-pairs is restricted to sign TLs only, an X.509 v3 certificate should include the following key purpose id OID in the extended key usage extension:

```
-- OID for TSL signing KeyPurposeID for ExtKeyUsageSyntax

   id-tsl OBJECT IDENTIFIER { itu-t(0) identified-organization(4)
                  etsi(0) tsl-specification (2231) }
   id-tsl-kp OBJECT IDENTIFIER ::= { id-tsl kp(3) }
   id-tsl-kp-tslSigning OBJECT IDENTIFIER ::= { id-tsl-kp tsl-signing(0) }
```

Additional general requirements regarding this signature are stated in the following clauses.

5.7.2 Signature algorithm identifier

Presence:	This field shall be present.
Description:	It specifies the cryptographic algorithm that has been used to create the signature. Depending on the algorithm used, this field may require additional parameters.
Format:	Character string or Bit string is suggested, depending on the implementation.
Value:	This field shall be included in the calculation of the signature.

5.7.3 Signature value

Presence: This field shall be present.

Description: It contains the actual value of the digital signature.

Value: All fields of the TL except the signature value itself shall be included in the calculation of the signature.

6 Operations

6.1 TL publication

TL Scheme Operators shall make TLs available through the Hypertext Transfer Protocol (HTTP) defined in RFC 2616 [8]. TLSOs may in addition support publication through LDAP, or FTP.

The HTTP URI pointing to the TL shall contain a fully qualified domain name in the host section, shall contain an absolute path and shall not contain a query section. The absolute path shall end with the string ".xml" or ".xtsl". There shall not be any extraneous header or trailer information in the file.

TLSOs shall publish, at the same locations they publish their trusted list, a digest that shall be computed as the SHA-256 hash value [11] of the binary representation of the trusted list as it can be retrieved by the server resolving the HTTP URI. The digest shall be published at an HTTP URI derived from the TL URI replacing the ".xml" or ".xtsl" string at the end of the absolute path with ".sha2".

This digest may be used to detect if an updated TL was published and shall not be used to authenticate the TL. Applications should regularly check for publication of a new version of a TL and not wait until the time contained in the Next update field (clause 5.3.15) of the previous TL or the previously downloaded TL is elapsed.

For example, the TLSOx's TL published at the location http://www.TLSOx.xyz/TrustedList/TL.xml is accompanied by its sha2 digest file i.e. on location http://www.TLSOx.xyz/TrustedList/TL.sha2. Downloaders may adopt the following strategy for downloading file TL.xml:

- check whether TL.sha2 is available for download:
  - if TL.sha2 has been successfully downloaded, verify the digest against the cached TL.xml file. If different, download and process TL.xml;
  - if TL.sha2 has not been successfully downloaded, download and process TL.xml directly.
- TL.xml should be downloaded/processed anyway if the nextUpdate (in the cached file) has been reached.

6.2 Transport Protocols

6.2.1 HTTP-Transport

This clause specifies a means for transport of TLs via the Internet using HTTP.

6.2.1.1 HTTP-Media Type

TL payloads shall be sent using the following media type:

- application/vnd.etsi.tsl+xml

The client may, when sending requests, provide an HTTP Accept header field. This header field should indicate an ability to accept "*application/vnd.etsi.tsl+xml*".

6.2.2 MIME registrations

A MIME-Type and a file-extensions support the transfer of TLs:

MIME media type name:	Application
MIME subtype name:	vnd.etsi.tsl+xml
Required parameters:	none
encoding considerations:	binary
File extension:	xml or xtsl
Security considerations:	TLs do not contain any active code or invoke any automated processing by itself. It is expected that clients only parse the TL and that there is no security risk. TLs are signed; no additional integrity protection is required. TLs typically are meant to be public, no confidentiality is required.
Published specification:	The TL format as defined in the present document.

6.3 TL Distribution Points in trust service tokens

Trust Service Providers may wish to give information on how to locate a TL of the scheme they operate under. To do so, they may include an appropriate extension in their trust service tokens (e.g. certificates, CRLs, time stamp tokens, OCSP responses and other). If such extension mechanism allows for the expression of criticality, this extension should not be marked critical. A distribution point should remain accessible until all trust service tokens it is referenced in have expired. The TSP shall guarantee that the distribution point in each trust service token is always resolved to the latest available applicable TL or to a scheme including a pointer to it (e.g. LOTL).

6.4 TL availability

TLSOs shall make their TLs available 24 hours a day and 7 days a week, with an availability percentage of minimum 99,9 % over one year.

6.5 TLSO practices

The TLSO shall define, maintain and implement appropriate measures, practices and policies, including change management and security procedures, for establishing, publishing and maintaining the trusted list to ensure that the information provided in the trusted list is timely, accurate, complete and authentic.

Annex A (informative): Authenticating and Trusting Trusted Lists

A.1 Authenticating and Trusting a TL

A TL is a signed data object. To verify the signature, relying parties need to be able to access the applicable public key. Since the scheme issuing the TLs 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.

In the case where several TLs participate to the same global approval scheme or participate to a common approval scheme or when there is a need to group and facilitate access to such TLs, a compiled list of pointers towards such TLs may be established, published and maintained. This compiled list of pointers can be designed on the model of "EUlistofthelists" type as specified in clause 5.3.3.

NOTE 1: 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. The "EUlistofthelists" type of such a LOTL is defined in clause D.5.

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

NOTE 2: The European Commission LOTL plays an important role in authenticating and trusting EU MS trusted lists. Each national trusted list is electronically signed by its scheme operator and the certificate to be used to verify such a signature is included in the LOTL after notification to the European Commission. The public key certificate(s) corresponding to the private key(s) entitled to be used to sign MS trusted lists and hence to be used by relying parties to validate those TLs signatures are published in the LOTL. The authenticity and integrity of the machine processable version of the LOTL is ensured through a qualified electronic signature supported by a qualified certificate which can be authenticated and directly trusted through one of the digests published in the Official Journal of the European Union (OJEU).

See https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers.

NOTE 3: Additionally the certificate(s) of the LOTL scheme operator is(are) included in any EU MS trusted list.

NOTE 4: In order to authenticate and trust an EU Member State trusted list, relying parties may:

1) download the LOTL from the protected location published in the OJEU, after having authenticated the trusted channel on the basis of the trusted channel certificate whose digest is published in the OJEU;

2) validate the signature on the downloaded LOTL, once having verified that the digest of the LOTL scheme operator public key certificate to be used to validate the signature maps one of the digests of the public key certificate(s) corresponding to the private key(s) entitled to be used to sign the LOTL as published in OJEU;

3) verify, once the LOTL signature being validated, the continued validity of the LOTL, by ensuring that the validity period of the LOTL has not expired;

4) parse the LOTL to retrieve the location and authentication information with regards to the target MS trusted list (one or more public key certificates may be associated to a MS TL as the public key certificate(s) corresponding to the private key(s) entitled to be used to sign the TL);

5) download the target MS TL;

6) validate the signature on the target MS TL, once having verified that the digest of the TL scheme operator public key certificate to be used to validate the signature maps one of the digests of the public key certificate(s) corresponding to the private key(s) entitled to be used to sign the target TL as published in the LOTL.

If either of the above checks fails, the TL authentication fails.

The procedure described above may be performed by each user, but will in many cases be carried out on the level of an organization according to their own policy. In this case, the software environment of each user's machine would typically be pre-configured and updated by the system administration or by the security officer. In time it is likely and certainly possible that such TLSOs or LOTL scheme operators certificates or public keys could also be pre-installed and updated in browsers, so enabling personal users to gain advantage from this approach.

A.2 Ensuring continuity in TL authentication

In order to ensure continuity in TL authentication, TL scheme operators should make sure that at all times two or more scheme operator public key certificates, with shifted validity periods, corresponding to the private keys entitled to be used to sign the TL are available in a trustworthy manner to relying parties (e.g. published in the LOTL in the context of EUMS TLs, or in an Official Journal). Those certificates may be issued so that they:

- do not have the same or too close validity start and end dates;
- are created on new key pairs as no previously used key pair are to be re-certified;
- are allocated to two or more scheme operator trustees in accordance with the scheme operator applicable policy; and
- are notified in due time to relying parties (e.g. to the EC for inclusion in the LOTL in the context of EUMS TLs).

In the case of compromise or decommissioning of one trusted list signature private key, TL scheme operators:

- when the current (into force) TL was signed with such a compromised or decommissioned private key, should re-issue, without any delay, a new trusted list signed with a non-compromised private key entitled to be used to sign the TL and whose corresponding public key certificate was already made available in a trustworthy manner to relying parties (e.g. is published in the LOTL);
- should promptly notify to the relying parties in a trustworthy manner:
  - of such a key compromise or decommissioning and the associated circumstances or reasons; and
  - a new list of public key certificate(s) corresponding to the private key(s) entitled to be used to sign the TL.

In the case of compromise (or decommissioning) of all the signature private keys corresponding to the public key certificates that were entitled to be used to validate one TL and were available to relying parties (e.g. published in the LOTL), scheme operators:

- should generate new key pairs and public key certificates corresponding to the private keys to be entitled to be used to sign the TL;
- should re-issue, without any delay, a new trusted list signed with one of those new private keys entitled to be used to sign the TL and whose corresponding public key certificate is to be made available in a trustworthy manner to relying parties;
- should promptly notify to the relying parties in a trustworthy manner:
  - of a such a key compromise; and
  - the new list of public key certificates corresponding to the private keys entitled to be used to sign the TL.

In the case of compromise or decommissioning of one signature private key related to a compiled list of pointers to several TLs, the compiled list scheme operator:

- when the current (into force) compiled list was signed with such a compromised or decommissioned private key, should re-issue, without any delay, a new compiled list signed with a non-compromised private key entitled to be used to sign the compiled list and whose corresponding public key certificate is published e.g. in an official journal;
- should promptly publish, e.g. in an official journal, a new list of public key certificate(s) corresponding to the private key(s) entitled to be used to sign the compiled list;
- should inform relying parties and stakeholders of such an official publication update together with the associated circumstances or reasons for such an update.

In the case of compromise (or decommissioning) of all compiled list signature private keys corresponding to the public key certificates entitled to be used to sign the compiled list and published, e.g. in an official journal, the compiled list scheme operator:

- should generate new key pairs and public key certificates corresponding to the private keys to be entitled to be used to sign the compiled list;
- should re-issue, without any delay, a new compiled list signed with one of those new private keys entitled to be used to sign the compiled list and whose corresponding public key certificate is to be published, e.g. in an official journal;
- should promptly publish, e.g. in an official journal, the new list of public key certificates corresponding to the private keys entitled to be used to sign the compiled list, deprecating compromised or decommissioned certificates;
- should inform the relying parties and stakeholders of such an official publication update together with the associated circumstances or reasons for such an update.

In the context of the direct trust model underlying their trustworthiness recognition, the revocation of TLSO and compiled list scheme operator certificate(s) are de facto implemented by the fact that the issuance of a new update of the related TL or compiled list deprecates the updated one and the deprecation of the compromised or decommissioned certificate(s) respectively in the compiled list and/or in the related official publication.

Annex B (normative): Implementation in XML

A TL shall comply with the XML schemas attached to the present document as part of a ZIP file identified in clause C, each one defining elements and types in a different namespace, respectively:

- http://uri.etsi.org/02231/v2#
- http://uri.etsi.org/TrstSvc/SvcInfoExt/eSigDir-1999-93-EC-TrustedList/#
- http://uri.etsi.org/02231/v2/additionaltypes#

NOTE: "02231" in the name space does not correspond to the ETSI document number of the present document because the name space was initially defined in TS 102 231 [i.6]. The previously defined name space is kept for compatibility reasons.

Applications shall use UTF-8 encoding for XML TLs.

With regards to the ElectronicAddressType type, the contents of each URI element shall represent a RFC 5322 [10] e-mail address, expressed by using the "mailto:" URI scheme as defined by RFC 2368 [7], or a web site address.

Processing of Critical attribute shall be as the one defined by RFC 5280 [13] for the critical field of extensions of X.509 v3 certificates. Applications shall reject the TL if they encounter a critical extension that they do not recognize. However, they may ignore a non-critical extension that they do not recognize.

B.1 The `Signature` element

Clause 5.7 requires that the TL is electronically signed: this includes use of XAdES [3] signatures (see annex F for further discussion). The TL-structure contains a `ds:Signature` element that represents an enveloped signature-type. The present document mandates the following constraints to any XML-Signature [5]-based signature applied to a TL:

1) It shall be an enveloped signature.

2) Its `ds:SignedInfo` element shall contain a `ds:Reference` element with the URI attribute set to a value referencing the `TrustServiceStatusList` element enveloping the signature itself. This `ds:Reference` element shall satisfy the following requirements:

   a) It shall contain only one `ds:Transforms` element.

   b) This `ds:Transforms` element shall contain two `ds:Transform` elements. The first one will be one whose `Algorithm` attribute indicates the enveloped transformation with the value: "http://www.w3.org/2000/09/xmldsig#enveloped-signature". The second one will be one whose Algorithm attribute instructs to perform the exclusive canonicalization "http://www.w3.org/2001/10/xml-exc-c14n#".

3) ds:CanonicalizationMethod shall be "http://www.w3.org/2001/10/xml-exc-c14n#".

4) It may have other `ds:Reference` elements.

NOTE 1: Rules 2 and 3 ensure that the enveloping `TrustServiceStatusList` element is actually signed as mandated by the processing model in clause 4.3.3.3 of XML-Signature [5] (with reference to same-document URI references). They also ensure that if relative referencing mechanisms are used in the `ds:Reference` element, the `TrustServiceStatusList` may be safely inserted within other xml documents.

NOTE 2: Rule 4 allows, among other things, for inclusion of signed properties in the signature, like the ones standardized in XAdES [3].

B.1.1 The scheme operator identifier in XAdES signatures

XAdES [3] defines the `xades:SigningCertificate` as a signed property that contains an identifier of the signer's certificate and its digest. This is therefore an effective way of securing the scheme operator identifier.

Even when the `xades:SigningCertificate` property is present, the present document does not prevent the inclusion of any of the three elements mentioned in the previous clause within the `ds:KeyInfo`'s child element `ds:X509Data`.

Should a `ds:X509Certificate` containing the signer's certificate be present within a XAdES signature as a child of a `ds:X509Data` within `ds:KeyInfo`, its serial number and issuer identifier shall match the serial number and issuer identifier present in the `xades:SigningCertificate` signed property.

Should the child of ds:X509Data element be a `ds:X509SKI` or an element encapsulating a public key, its contents shall be consistent with the contents of the `xades:SigningCertificate` signed property, if present.

B.1.2 Algorithm and parameters

The algorithms, their parameters and formats supported by the present document shall be:

- those supported by XML-Signature [5]; or
- the Elliptic Curve Digital Signature Algorithm (ECDSA) as defined in [i.4]; or
- the SHA-2 algorithms as defined in [11].

Annex C (normative): XML schema

C.1 Electronic attachment

The present document has an associated electronic ZIP file "ts_119612v010201p0.zip" that contains the XML schemas that are integral parts of the present document and further described below.

In the event that any part of the module and/or schemas within this electronic attachment are in conflict with the text of the present document, the present document shall prevail as the authoritative source.

C.2 XML schemas

The XML schemas are held in the following files:

1) "ts_119612v010201_xsd.xsd" containing the base schema definitions. For the purpose of integrity checking, the hash values of this file are:

   SHA-1: 7b:f0:c6:6b:0b:a2:21:40:f5:ff:90:50:f6:ba:6e:35:d7:48:7a:c8

   SHA-256: 18:3d:4b:39:17:64:46:3b:f1:07:64:63:f2:89:b5:9b:05:ca:77:22:57:19:10:a3:6d:1d:cf:eb:3b:4d:b4:f4

2) "ts_119612v010201_sie_xsd.xsd" containing the schema definitions for additional service information extensions (clause D.5). For the purpose of integrity checking, the hash values of this file are:

   SHA-1: 43:4c:4e:3a:fd:bd:1a:24:23:d9:ff:69:95:c1:20:26:fb:6e:ec:4b

   SHA-256: 1e:7c:c7:32:62:32:28:39:c7:ab:e1:cb:b1:3a:75:64:8f:5e:c4:28:9d:37:67:78:4e:4d:47:6a:40:dd:96:e5

3) "ts_119612v010201_additionaltypes_xsd.xsd" containing the schema definitions for additional types. For the purpose of integrity checking, the hash values of this file are:

   SHA-1: a3:9c:f4:e6:bd:1e:4f:a4:9d:ca:fd:1b:2a:68:f1:09:f7:f4:54:03

   SHA-256: 18:9e:e4:91:d1:72:da:a1:0f:a0:21:c1:cb:d1:f2:12:b2:2c:ee:8c:6a:f0:b8:6e:47:28:be:b5:aa:2a:eb:ea

Annex D (normative): Registered Uniform Resource Identifiers

This annex specifies those Uniform Resource Identifiers (URIs) which have been registered in connection with the present document. Those with the radix (base) "http://uri.etsi.org/19612/……" are registered and declared by their presence in the present document, for specific usage within the present document: those with the radix "http://uri.etsi.org/TrstSvc/……" are registered by ETSI as a Common Domain (see http://portal.etsi.org/pnns/xml.asp#Common_Domain) on behalf of the TC ESI because they have a wider applicability and usage and are defined in the present document.

In the following tables the following layout is used for each URI declaration:

The URI is given as an unbroken string	Related TSL field (if any)
The meaning of the URI is given, indented to emphasize its relationship to the preceding URI.	

Where more than one URI relates to a specific TL field the second column will extend across all URI declarations (row-pairs) which apply.

D.1 URIs registered within the present document

The following URIs are hereby declared and registered under the present document's assigned radix:

http://uri.etsi.org/19612/v1.1.1	N/a
This issue of TS 119 612 and its related parts.	

http://uri.etsi.org/19612/TSLTag	TSL tag
A data structure which conforms to the TSL specification published in TS 119 612 in any of its historical issues or this one.	

http://uri.etsi.org/02231/v2#	N/a
The XML namespace identifier relating to the TSL version specified in this issue of TS 119 612.	

http://uri.etsi.org/19612/TDPContainer	N/a
A qualifier for web pages that contain one or more TDPs which can be used as a value of the attribute "profile" for the "head" element of the web page.	

D.2 ETSI Common Domain URIs

The following URIs have been declared and registered by ETSI under the Technical Committee Electronic Signatures Infrastructure's (TC ESI) assigned radix.

D.2.1 Service Type

http://uri.etsi.org/TrstSvc/Svctype/CA/PKC	Service type identifier
A certificate generation service creating and signing non-qualified public key certificates based on the identity and other attributes verified by the relevant registration services.	
http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
A certificate generation service creating and signing qualified certificates based on the identity and other attributes verified by the relevant registration services.	
http://uri.etsi.org/TrstSvc/Svctype/TSA	
A time-stamping generation service creating and signing time-stamps tokens.	
http://uri.etsi.org/TrstSvc/Svctype/TSA/QTST	
A time-stamping generation service creating and signing qualified time-stamps tokens.	
http://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-QC	
A time stamping service as part of a service from a trust service provider issuing qualified certificates that issues time-stamp tokens (TST) that can be used in the validation process of qualified signature or advanced signatures supported by qualified certificates to ascertain and extend the signature validity when the qualified certificate is (will be) revoked or expired (will expire).	
http://uri.etsi.org/TrstSvc/Svctype/TSA/TSS-AdESQCandQES	
A time stamping service as part of a service from a trust service provider that issues time-stamp tokens (TST) that can be used in the validation process of qualified signature or advanced signatures supported by qualified certificates to ascertain and extend the signature validity when the qualified certificate is (will be) revoked or expired (will expire).	
http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP	
A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses.	
http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC	
A certificate validity status services issuing Online Certificate Status Protocol (OCSP) signed responses and operating an OCSP-server as part of a service from a trust service provider issuing qualified certificates.	
http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL	
A certificate validity status services issuing CRLs.	
http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL/QC	
A certificate validity status services issuing CRLs.	
http://uri.etsi.org/TrstSvc/Svctype/RA	
A registration service that verifies the identity and, if applicable, any specific attributes of a subject for which a certificate is applied for, and whose results are passed to the relevant certificate generation service.	
http://uri.etsi.org/TrstSvc/Svctype/RA/nothavingPKIid	
A registration service that verifies the identity and, if applicable, any specific attributes of a subject for which a certificate is applied for, and whose results are passed to the relevant certificate generation service. Such a registration service cannot be identified by a specific PKI-based public key.	

http://uri.etsi.org/TrstSvc/Svctype/ACA	
An attribute certificate generation service creating and signing attribute certificates based on the identity and other attributes verified by the relevant registration services.	
http://uri.etsi.org/TrstSvc/Svctype/SignaturePolicyAuthority	
A service responsible for issuing, publishing or maintenance of signature policies.	
http://uri.etsi.org/TrstSvc/Svctype/NationalRootCA-QC	
A national root signing CA issuing root-signing or qualified certificates to trust service providers and related certification or trust services that are accredited against a national voluntary accreditation scheme or supervised under national law in accordance with the applicable European legislation.	
http://uri.etsi.org/TrstSvc/Svctype/Archiv	
An Archival service.	
http://uri.etsi.org/TrstSvc/Svctype/REM	
A Registered Electronic Mail service.	
http://uri.etsi.org/TrstSvc/Svctype/EDS	
An electronic delivery service.	
http://uri.etsi.org/TrstSvc/Svctype/EDS/Q	
An electronic delivery service providing qualified electronic deliveries.	
http://uri.etsi.org/TrstSvc/Svctype/PSES	
A preservation service for electronic signatures.	
http://uri.etsi.org/TrstSvc/Svctype/PSES/Q	
A preservation service for qualified electronic signatures.	
http://uri.etsi.org/TrstSvc/Svctype/IdV	
An Identity verification service.	
http://uri.etsi.org/TrstSvc/Svctype/KEscrow	
A Key escrow service.	
http://uri.etsi.org/TrstSvc/Svctype/PPwd	
Issuer of PIN- or password-based identity credentials.	
http://uri.etsi.org/TrstSvd/Svctype/TLIssuer	
A service issuing trusted lists.	
http://uri.etsi.org/TrstSvc/Svctype/unspecified	
A trust service of an unspecified type.	

D.3 Scheme registered URIs

Any organization operating a scheme might choose to create its own URIs for its own specific purposes or request ETSI to assign a registered URI root under the ETSI Identified Organization Domain (see http://portal.etsi.org/pnns/xml.asp), and then define its own URIs under this root. It might be appropriate to register certain of those URIs where they complement URIs required by or which might be used in the context of the publication of a TL. The following examples suggest how additional URIs could be created, including showing a second level of rules, after using the applicable Optional URI as shown above:

Potential URI **Meaning**	**Related TSL field (if any)**
http://uri.etsi.org/"registered_org"/"schemename"	Scheme type/community/rules (at the secondary level)
This could mean an assessment scheme called "schemename" being operated by "registered_org", where "registered_org" is replaced by the name of the scheme operator and "schemename" is replaced by the actual scheme name.	
http://"scheme_op_URI_root"/.../schemerules/ "schemename"	
This URI would be registered under a different root, e.g. the scheme operator's, distinguished by "scheme_op_URI_root", or it could be another organization which maintains a registry of URIs. This URI could mean an assessment scheme called "schemename" being operated by "scheme_op" where "scheme_op" is replaced by the name of the scheme operator and "schemename" is replaced by the actual scheme name.	

D.4 Common Trusted Lists URIs

The following URIs, are registered under the radix "http://uri.etsi.org/TrstSvc/TrustedList/":

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC where CC is replaced with the code used in the "Scheme territory" field (see clause 5.3.10).	Scheme type/community/rules
A URI specific to CC's trusted list pointing towards a descriptive text that shall be published by the TLSO and applicable to this CC's trusted list: • Where users can obtain the referenced CC's specific policy/rules against which services included in the list shall be assessed in compliance with the CC's appropriate approval schemes. • Where users can obtain a referenced CC's specific description about how to use and interpret the content of the trusted list (e.g. in the EU with regard to the trust services not related to the issuing of qualified certificates, where this may be used to indicate a potential granularity in the national supervision/accreditation systems related to trust service providers not issuing qualified certificates and how the "Scheme service definition URI" (see clause 5.5.6) and the "Service information extension" field (see clause 5.5.9) are used for this purpose).	

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/RootCA-QC	Service information extensions/additionalServiceInformation Extension/
A Root Certification Authority from which a certification path can be established down to a Certification Authority issuing qualified certificates. This value shall not be used if the service type is not http://uri.etsi.org/TrstSvc/Svctype/CA/QC	

D.5 EU specific Trusted Lists URIs

The following URIs, are registered under the radix "http://uri.etsi.org/TrstSvc/TrustedList/":

http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric	TSL type
A TL implementation of a supervision/accreditation status list of trust services from trust service providers which are supervised/accredited by the referenced Member State owning the TL implementation for compliance with the relevant provisions laid down in the applicable European legislation, through a process of direct oversight (whether voluntary or regulatory).	
http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists	
A TL implementation of a compiled list of pointers towards Member States supervision/accreditation status lists of trust services from trust service providers which are supervised/accredited by the referenced Member State owning the pointed TL implementation for compliance with the relevant provisions laid down in the applicable European legislation, through a process of direct oversight (whether voluntary or regulatory).	

http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/EUappropriate	Status determination approach (see below the section Supervision/accreditation status flow)
Services listed have their status determined by or on behalf of the Scheme Operator under an appropriate system as defined by the Member State implementation of the applicable European legislation and further described in the 'Scheme information URI' pointed-to information.	

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUlistofthelists	Scheme type/community/rules
A URI pointing towards a descriptive text where users can obtain information about the scheme of schemes type (i.e. a compiled list listing pointers to all trusted lists published as part of the scheme of schemes and maintained in the form of a TL) and the relevant driving rules and policy.	
http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon	
A URI pointing towards a descriptive text that applies to all EU Member States' trusted lists: • By which participation of the Member States' trusted lists is denoted in the general scheme of the EU Member States trusted lists. • Where users can obtain policy/rules against which services included in the trusted list are assessed. • Where users can obtain description about how to use and interpret the content of the EU Member States' trusted list. These usage rules are common to all EU Member States' trusted lists whatever the type of listed services.	

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCWithSSCD	Service information extensions/Qualifications Extension/Qualifiers
QCWithSSCD it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that **all Qualified Certificates** issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support **ARE supported by an SSCD** (i.e. that that the private key associated with the public key in the certificate is stored in a Secure Signature Creation Device conformant with the applicable European legislation); This value shall not be used if the service type is not http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCNoSSCD	
QCNoSSCD it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that **all Qualified Certificates** issued under the service identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support **ARE NOT supported by an SSCD** (i.e. that that the private key associated with the public key in the certificate is not stored in a Secure Signature Creation Device conformant with the applicable European legislation). This value shall not be used if the service type is not http://uri.etsi.org/TrstSvc/Svctype/CA/QC	
http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCSSCDStatusAsInCert	
QCSSCDStatusAsInCert it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that **all Qualified Certificates** issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the presence or absence of Secure Signature Creation Device (SSCD) support **DO contain the machine-processable information indicating whether or not the Qualified Certificate is supported by an SSCD**. This value shall not be used if the service type is not http://uri.etsi.org/TrstSvc/Svctype/CA/QC.	
http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCForLegalPerson	
QCForLegalPerson it is ensured by the trust service provider and controlled (supervision model) or audited (accreditation model) by the referenced Member State (respectively its Supervisory Body or Accreditation Body) that **all Qualified Certificates** issued under the service (RootCA/QC or CA/QC) identified in "Service digital identity" and further identified by the filters information used to further identify under the "Sdi" identified trust service that precise set of Qualified Certificates for which this additional information is required with regards to the issuance to Legal Person **ARE issued to Legal Persons**. This value shall not be used as an extension, if the service type is not http://uri.etsi.org/TrstSvc/Svctype/CA/QC	

http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCStatement	
QCStatement it is ensured by the CSP and controlled (supervision model) or audited (accreditation model) by the Member State (respectively its Supervisory Body or Accreditation Body) that **all certificates** issued under the service (CA/QC) identified in 'Service digital identity' (clause 5.5.3) and further identified by the above (filters) information used to further identify under the 'Sdi' identified trust service that precise set of certificates for which this additional information is required with regard to the issuance of such certificates **is issued as a Qualified Certificate.** This value shall not be used as an extension, if the service type is not http://uri.etsi.org/TrstSvc/Svctype/CA/QC	

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision	Service current status (excepted for NationalRootCA-QC type)
Under Supervision The service identified in "Service digital identity" (see clause 5.5.3) provided by the trust service provider identified in "TSP name" (see clause 5.4.1) is currently under supervision, for compliance with the provisions laid down in the applicable European legislation, by the Member State identified in the "Scheme territory" (see clause 5.3.10) in which the trust service provider is established.	
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation	
Supervision of Service in Cessation The service identified in "Service digital identity" (see clause 5.5.3) provided by the trust service provider identified in "TSP name" (see clause 5.4.1) is currently in a cessation phase but still supervised until supervision is ceased or revoked. In the event a different person than the one identified in "TSP name" has taken over the responsibility of ensuring this cessation phase, the identification of this new or fallback person (fallback trust service provider) shall be provided in "Scheme service definition URI" (clause 5.5.6) and in the "TakenOverBy" extension (clause 5.5.9.3) of the service entry. "Supervision of Service in Cessation" status shall be used when a TSP directly ceases its related services under supervision; it shall not be used when supervision has been revoked.	
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionceased	
Supervision Ceased The validity of the supervision assessment has lapsed without the service identified in "Service digital identity" (see clause 5.5.3) being re-assessed. The service is currently not under supervision any more from the date of the current status as the service is understood to have ceased operations. "Supervision Ceased" status shall be used when a TSP directly ceases its related services under supervision; it shall not be used when supervision has been revoked.	
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionrevoked	
Supervision Revoked Having been previously supervised, the trust service provider's service and potentially the trust service provider itself has failed to continue to comply with the provisions laid down in the applicable European legislation, as determined by the Member State identified in the "Scheme territory" (see clause 5.3.10) in which the trust service provider is established. Accordingly the service has been required to cease its operations and shall be considered by relying parties as ceased for the above reason. The status value "Supervision Revoked" may be a definitive status, even if the trust service provider then completely ceases its activity; it shall not be migrated (without any intermediate status) to either "Supervision of Service in Cessation" or to "Supervision Ceased" status in this case. The only way to change the "Supervision Revoked" status is to recover from non-compliance to compliance with the provisions laid down in the applicable European legislation according the appropriate supervision system in force in the Member State owing the trusted list, and regaining "Under Supervision" status. "Supervision of Service in Cessation" status, or "Supervision Ceased" status shall be used when a TSP directly ceases its related services under supervision; they shall not be used when supervision has been revoked.	

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accredited	
Accredited An accreditation assessment has been performed by the Accreditation Body on behalf of the Member State identified in the "Scheme territory" (see clause 5.3.10) and the service identified in "Service digital identity" (see clause 5.5.3) provided by the trust service provider identified in "TSP name" (see clause 5.4.1) is found to be in compliance with the provisions laid down in Directive 1999/93/EC [i.3]. This accredited trust service provider may be established in another Member State than the one identified in the "Scheme territory" (see clause 5.3.10) of the trusted list or in a non-EU country (see article 7.1(a) of Directive 1999/93/EC [i.3]).	
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationceased	
Accreditation Ceased The validity of the accreditation assessment has lapsed without the service identified in "Service digital identity" (see clause 5.5.3) being re-assessed.	
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/accreditationrevoked	
Accreditation Revoked Having been previously found to be in conformance with the scheme criteria, the service identified in "Service digital identity" (see clause 5.5.3) provided by the trust service provider identified in "TSP name" (see clause 5.4.1) and potentially the trust service provider itself have failed to continue to comply with the provisions laid down in Directive 1999/93/EC [i.3].	

Supervision/accreditation status flow

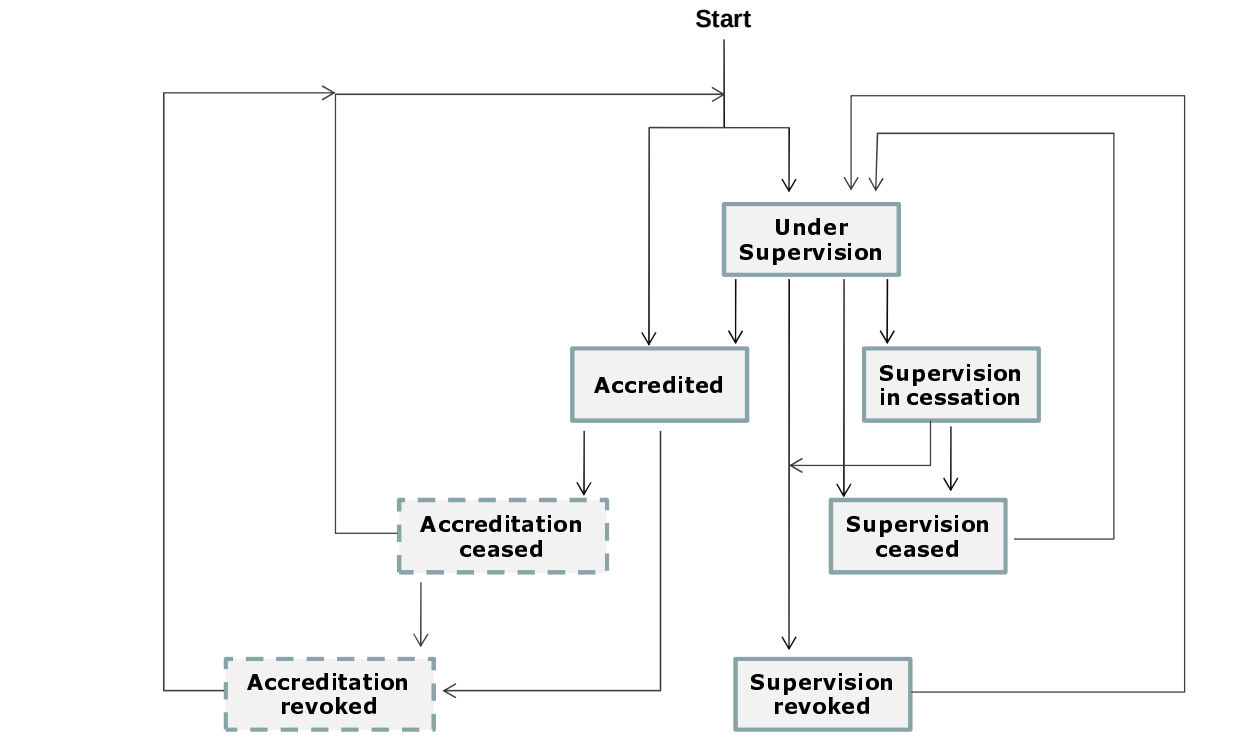

Figure D.1: Supervision/accreditation status flow

http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/setbynationallaw	Service current status (for NationalRootCA-QC type only)
Set by national law The service is set by national law in accordance with the applicable European legislation and operated by the responsible national body issuing root-signing or qualified certificates to accredited trust service providers.	
http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/deprecatedbynationallaw	
Deprecated by national law The service is deprecated by national law in accordance with the applicable European legislation and by the responsible national body issuing root-signing or qualified certificates to accredited trust service providers.	

D.6 Non-EU specific Trusted Lists URIs

The following URIs, are registered under the radix "http://uri.etsi.org/TrstSvc/……":

http://uri.etsi.org/TrstSvc/TrustedList/TSLType/CClist where "CC" is replaced by a character string identifying the community to which it applies (e.g. "ASEAN", "GCC" or the ISO 3166-1 [16] alpha-2 Country Code used in the 'Scheme territory field' (clause 5.3.10)).	TSL type
Indicates a trusted list providing assessment scheme based approval status information about trust services from trust service providers which are approved by the competent trusted list scheme operator or by the State or body in charge from which the scheme operator depends or by which it is mandated, for compliance with the relevant provisions of the applicable approval scheme and/or the applicable legislation.	
http://uri.etsi.org/TrstSvc/TrustedList/TSLType/CClistofthelists where "CC" is replaced by a character string identifying the community to which it applies (e.g. "ASEAN", "GCC" or the ISO 3166-1 [16] alpha-2 Country Code used in the 'Scheme territory field' (clause 5.3.10)).	
Indicates a compiled list of pointers towards community members' lists of trust services from trust service providers which are approved by the competent trusted list scheme operator or by the State or body in charge from which the scheme operator depends or by which it is mandated, for compliance with the relevant provisions of the applicable approval scheme and/or the applicable legislation.	

http://uri.etsi.org/TrstSvc/TrustedList/StatusDetn/CCdetermination where "CC" is replaced by a character string identifying the community to which it applies (e.g. "ASEAN", "GCC" or the ISO 3166-1 [16] alpha-2 Country Code used in the 'Scheme territory field' (clause 5.3.10).	Status determination approach
Services listed have their status determined after assessment by or on behalf of the scheme operator against the scheme's criteria (active approval/recognition) and as further described in the 'Scheme information URI' pointed-to information.	

Annex E (normative): Implementation requirements for multilingual support

E.1 General rules

When establishing their trusted lists, TLSOs shall use:

- Language codes in lower case and country codes in upper case.
- Language and country codes according to table E.1 with regards to EU MS.

When a Latin script is present (with its proper language code) a transliteration in Latin script with the related language codes specified in table E.1 is added.

Table E.1

Short name (source language)	Short name (English)	Country Code	Language Code	Notes	Transliteration in Latin script
Belgique/België	Belgium	BE	fr, de, nl		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Country code recommended by EU	el-Latn
España	Spain	ES	es	also Catalan (ca), Basque (eu), Galician (gl)	
France	France	FR	fr		
Hrvatska	Croatia	HR	hr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Country code recommended by EU	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

NOTE: (*) Latin transliteration: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

E.2 Multilingual character string

The string contained within a multilingual character string shall fulfil the requirements of annex N of ISO/IEC 10646 [6] subject to the following restrictions:

1) the content shall be a string of characters from the Universal Character Set (UCS) as defined by ISO/IEC 10646 [6];

2) the content shall be UTF-8 encoded;

3) the content shall not include any signature to identify the UCS (see annex H of ISO/IEC 10646 [6]);

4) control functions (ISO/IEC 6429 [14]), escape sequences (ISO/IEC 2022 [15]) and control sequences or strings shall not be used; therefore control characters such as TAB, CR, LF shall not be present;

5) private-use characters (see clause 10 of ISO/IEC 10646 [6]) from the private use zone (code points E000 to F8FF) in the Basic Multilingual Plane (BMP) and from the private-use Planes 0F and 10 in Group 00, shall not be used;

6) Tag Characters (see annex T of ISO/IEC 10646 [6]) shall not to be used: therefore the characters from the TAGS (3001) collection shall not be used (see annex A of ISO/IEC 10646 [6] for the list of defined collections);

7) the content shall be plain text without any mark-up elements or tags from languages as SGML, HTML, XML, XHTML, RTF, TeX and others;

8) the content should follow the semantic rules defined by the Unicode Standard (available at http://www.unicode.org/standard/standard.html) for the corresponding characters;

9) combining characters should not be used if the content can be expressed without them; if there is the need to use combining characters but it is possible not to use the ones listed in clause B.1 of ISO/IEC 10646 [6], then that latter set shall not be used.

NOTE: This helps to keep as low as possible the required implementation level (as defined by clause 14 of ISO/IEC 10646 [6]) for parsing applications.

E.3 Multilingual pointer

If the content pointed by the multilingual pointer is plain text, it shall meet the following requirements that express the conformity to annex N of ISO/IEC 10646 [6] and add further restrictions:

1) the pointed content shall be a string of characters from the Universal Character Set (UCS) as defined by ISO/IEC 10646 [6];

2) the pointed-to content shall be UTF-8 encoded;

3) the pointed-to content may include the signature for UTF-8 (see annex H of ISO/IEC 10646 [6]) to identify the UCS;

4) control functions (ISO/IEC 6429 [14]), escape sequences (ISO/IEC 2022 [15]) and control sequences or strings may be used;

5) private-use characters (see clause 10 of ISO/IEC 10646 [6]) from the private use zone (code points E000 to F8FF) in the Basic Multilingual Plane (BMP) and from the private-use Planes 0F and 10 in Group 00, shall **not** be used;

6) Tag Characters (see annex T of ISO/IEC 10646 [6]) shall not to be used: therefore the characters from the TAGS (3001) collection shall not be used (see annex A of ISO/IEC 10646 [6] for the list of defined collections);

7) if the pointed-to content is expressed by means of mark-up languages as SGML, HTML, XML, XHTML then:

   a) the requirements described in W3C Technical Report #20 [i.7] should be met;

   b) a language indication may be present according to the mechanisms listed in W3C Technical Report #20 [i.7].

8) the pointed-to content should follow the semantic rules defined by the Unicode Standard (available at http://www.unicode.org/standard/standard.html) for the corresponding characters;

9) combining characters should not be used if the pointed-to content can be expressed without them; if there is the need to use combining characters but it is possible not to use the ones listed in clause B.1 of ISO/IEC 10646 [6], then that latter set shall not be used.

NOTE: This helps to keep as low as possible the required implementation level (as defined by clause 14 of ISO/IEC 10646 [6]) for parsing applications).

E.4 Overall requirements

The requirements of W3C Technical Report #20 [i.7] should be met.

For interoperability purposes, all applications parsing TLs shall be able to store and manage all characters defined by ISO/IEC 10646 [6]. This way the digital signature applied to the TL can be always verified, whatever UCS characters are used within the TL. However the parsing application may not be able to correctly present all characters.

NOTE: Developers of TL parsing applications are advised that if their application does not support some of these characters, the application should give notice to the user about possible incorrect representation of the content of multilingual fields; the precise behaviour of the application while presenting unsupported characters is left to developers.

Annex F (informative): TL manual/auto field usage

Table F.1 lists all fields defined for the TL and indicates whether the field contents should be made available to users when presenting the TL in a human-readable form (column 2) or whether the field is considered to be essential for effective automatic parsing (column 3), noting that all fields will be accessible through an automated process.

Although this annex is informative implementers are strongly recommended to satisfy the guidance which it provides, in order to provide users with information about TLs in a consistent manner.

Table F.1

Field name	Human-readable?	Machine-processable?
Identification Tag		
TSL tag		✓
Scheme information		
TSL version identifier	✓	✓
TSL sequence number	✓	✓
TSL type	✓	✓
Scheme operator name	✓	
Scheme operator address	✓	
Scheme name	✓	
Scheme information URI	✓	✓
Status determination approach	✓	✓
Scheme type/community/rules	✓	✓
Scheme territory	✓	✓
TSL policy/legal notice	✓	✓
Historical information period	✓	✓
Pointers to other TSLs	✓	✓
List issue date and time	✓	✓
Next update	✓	✓
Scheme extensions	where recognized and meaningful	where recognized
TSP information		
TSP name	✓	
TSP trade name	✓	
TSP address	✓	
TSP information URI	✓	✓
TSP information extensions	where recognized and meaningful	where recognized
Service information		
Service type identifier	✓	✓
Service name	✓	
Service digital identity	✓	✓
Service current status	✓	✓
Current status starting date and time	✓	✓
Scheme service definition URI	✓	✓
Service supply points	✓	✓
TSP service definition URI	✓	✓
Service information extensions	where recognized and meaningful	where recognized
Historical service information		
Service type identifier	✓	✓
Service name	✓	
Service digital identity	✓	✓
Service previous status	✓	✓
Previous status starting date and time	✓	✓
Service information extensions	where recognized and meaningful	where recognized
TSL signature information		
Scheme identification		✓
Textual certificate details, time and date of signing	✓	✓
Cryptographic data		✓

Annex G (normative): Management and Policy considerations

Specific criteria for the provision of revisions to TL information apply. These revisions will fall into the following categories.

G.1 Change of scheme administrative information

This category includes any changes to information concerning the scheme and which is embedded within the TL. Such changes could include, *inter alia*, change of scheme addresses, revisions to acceptance criteria, scheme policy.

When these changes occur and are material changes to information included in the TL, the TL shall be re-issued.

NOTE: If there are material changes to information directly referenced through the TL but the reference itself does not change then there will be no need to amend the TL.

If the changes were the result of a change of ownership of the entity operating the scheme then the scheme should continue to operate with changes with regards to information related to the Scheme Operator and the TL being re-issued.

G.2 Trust-service identification

Whenever a scheme operator adds trust service to a TL, it is important to users of the TL to be able to unambiguously identify that service's status definition. While name and address may be highly relevant and therefore very important, the digital identity-field is the only option that can provide secure identification of the trust service and tokens which it supplies.

G.3 Change of trust service status

These changes are those directly affecting the inclusion or reported status of any trust service within the TL (and possibly also information concerning their provider) and whether the information is current or historical (e.g. the introduction of a new TSP and service; the revocation of a service).

When any such change occurs the TL shall be re-issued with the previous current status becoming the most recent historical status and current status being amended to reflect the situation.

The service which is effectively stopping should have its "Service current status" (see clause 6.4.4) revised to meaning "ceased" operations and the previous status information placed into the "History information" (see clause 6.5) of the TL. This shall then be retained for the published retention period (since there may be requirements to check on services rendered during its period of activity). No ceased service's "Historical information" shall be discarded.

G.4 Change in trust service digital identity

Where a service changes its "Service digital identity" (see clause 5.5.3):

- In the case of a new public key (e.g. as a result of a re-branding or a renewal of associated digital data for security reasons), the service related to the new digital identity (public key) shall be added in the TL as a new service entry. As new service, the "History information" is absent.
- In the case of a new certificate for the same public key (e.g. as a result of a re-branding or a renewal of associated digital data), a new "History information" field shall be added to the service approval history, and this new representation of the public key shall be added as part of the current status information.

G.5 Amendment response times

Changes to any TL information shall be provided in a timely fashion, not exceeding 24 hours.

In particular, once the decision to change the status of a listed certification or trust service is effective, the corresponding change should be implemented and the TL re-issued in less than four working hours.

G.6 On-going verification of authenticity

The frequency at which information within a TL will change is likely to be low. This could give a determined hacker sufficient time to replicate and replace all instances of a TL, *IF* they were able to replace all examples of the TL itself and a surrogate PKC for the TL scheme operator. This should be protected against by the scheme operator itself making frequent verification of its own TL and all authorized and recognized replications of it. In addition, the regular re-issuing of the TL, even when there is no change to any statuses within it, will also ensure that, at the least, the signature value changes periodically.

G.7 User reference to TL

Scheme operators should assist in this by offering additional services to notify when a new TL is issued, or to guarantee frequent re-issue of a TL at a frequency which may mean numerous re-issues without change of any services' status. However, the mechanisms proposed for having multiple copies of TLs existing contemporaneously are designed to cater for the low rate of information change already discussed, and these may not be suitable for frequent TL re-issue.

G.8 TL size

The present document provides a number of fields in which the scheme operator may choose to provide actual natural language text in preference to a URI or other reference to a source of information. Clearly the inclusion of large quantities of text will have a direct influence on download and parsing times, this especially so if e.g. it relates to the descriptions of services, and the scheme has a large number of trust services listed. Implementers should therefore take advantage of the opportunity to use URIs and limit embedded text as much as is reasonable, accounting for the overall size of the TL and the available bandwidth and storage capacities of the typical user of their TL. Referencing other documents also allows advantage to be taken of more sophisticated presentation options which formats such as PDF and other formats enable.

Annex H (informative): Locating a TL

H.1 Introduction

This annex provides guidance on how to locate TLs.

H.2 Locating a TL

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.

With regards to PKI based services, the country related information of the issuer of a trust service token (e.g. (qualified) certificates, time-stamping tokens, signed OCSP responses, signed CRLs) provides as hint the MS indication where the TL can be retrieved from.

Annex I (informative): Usage of Trusted Lists

I.1 Introduction

This annex describes an example of model for the usage of trusted lists. This model is not aimed to restrict how an implementation may be built but identifies the functionality that may be expected from systems applying trusted lists.

I.2 Example of model for the usage of Trusted Lists in the context of signature validation

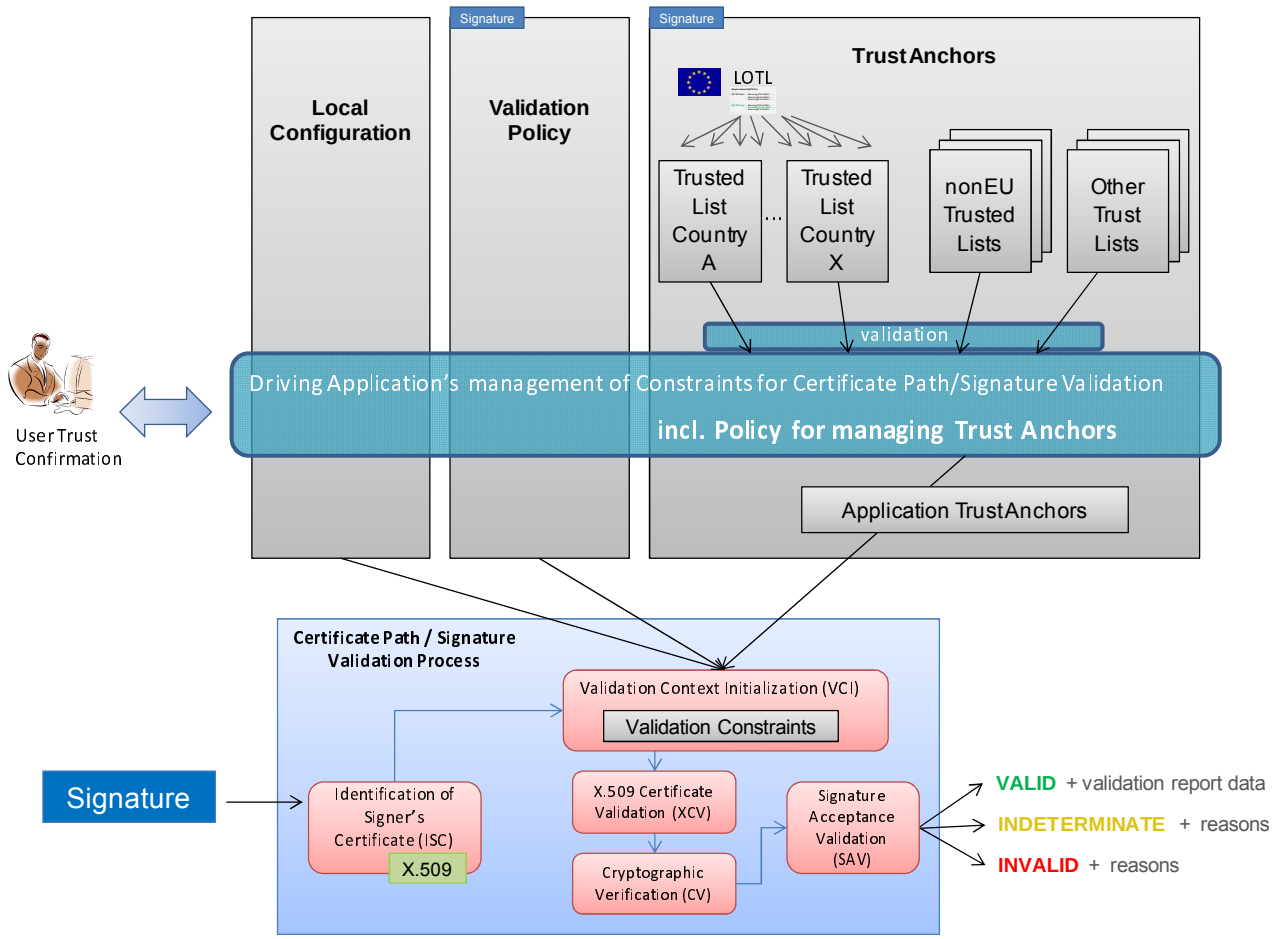

Figure I.1: Example of model for the usage of TL in the context of signature validation

Information from trusted lists may be used in the certificate path validation process for an application as follows:

- Certificate path validation based upon X.509 (see RFC 5280 [13]) or TS 102 853 [i.1] on signature verification requires information on CA certificates that can be used as trust anchors for an application requiring a particular Trust Service.

- When "Service digital identifiers" are to be used as Trust Anchors in the context of validating electronic signatures for which signer's certificate is to be validated against TL information, only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are considered as Trust Anchor certificates conveying identical information with regards to the information strictly required as Trust Anchor information.

This information can be derived from one or more trusted lists as follows:

a) The source of the trusted list is validated to ensure that the information comes from a trusted issuer (e.g. using a digital signature validated using a certificate known to come from a recognized authority).

b) CA entries are selected from the trusted list based on the rules of the applicable trust policy.

c) CA certificates from the selected entries, optionally with associated meta data, are held with the Trust Anchors.

d) The trusted list is checked regularly for changes to the service status of the CAs in the Trust Anchor store which were previously loaded from the trusted list. The trusted list is also regularly checked for new entries.

e) A human user or operator may be asked for confirmation before an entry is added to the Trust Anchors store.

f) CA information from multiple trusted lists may be loaded into the Trust Anchors store.

CA Information from trusted lists may be combined with CA information in the Trust Anchor store or from any trusted CA certificate store loaded by other means, manually or in an automated way.

I.3 Policy elements for Trust Anchor management

Policy elements for Trust Anchor management may specify the types, status and any other relevant properties of trust services or other trusted entities whose certificates are acceptable as Trust Anchors.

These policy elements may be defined, locally, for a community of users, by the application provider or by the system provider.

An example policy rule for an application that requires TSPs supervised or accredited for issuing qualified certificates in line with Directive 1999/93/EC [i.3] for qualified electronic signatures may be:

i) ServiceType equals: http://uri.etsi.org/TrstSvc/Svctype/CA/QC; and

ii) ServiceStatus is:

- **Under Supervision** (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/undersupervision); or
- **Supervision of Service in Cessation** (http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/supervisionincessation); or
- **Accredited** (http://uri.etsi.org/TrstSvc/Svcstatus/TrustedList/Svcstatus/accredited).

History

Document history		
V1.1.1	June 2013	Publication
V1.2.1	April 2014	Publication