ETSI TS 119 612 V2.1.1 (2015-07)

Electronic Signatures and Infrastructures (ESI); Trusted Lists

Reference

RTS/ESI-0019612v2

Keywords

e-commerce, electronic signature, security, trust services

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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).

Modal verbs terminology

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

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

Introduction

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 digital signatures and trust services for electronic transactions.

The present document is aiming to meet the general requirements of the international community to allow production of trusted list including information on qualified and non-qualified trust service providers and the qualified and non-qualified trust services they provide, including, amongst others, applicable requirements from Regulation (EU) No 910/2014 [i.10].

NOTE 1: EU Member States' trusted lists were established in EU by Commission Decision 2009/767/EC [i.2] and aimed primarily at supporting the validation of advanced electronic signatures supported by a qualified certificate and advanced electronic signature supported by both a qualified certificate and by a secure signature creation device, in the meaning of Directive 1999/93/EC [i.3], as far as they included as a minimum trust service providers supervised/accredited for issuing qualified certificates. TLSOs could however include in their trusted lists also other types of approved trust service providers. Hence, the cross-border use of electronic services based on advanced electronic signatures is also facilitated, where the supporting trust services (e.g. issuing of non-qualified certificates) are part of the listed supervised/accredited services.

Regulation (EU) No 910/2014 [i.10] extends the scope of qualified trust services and trust service providers to a wider but definite list of harmonised trust services. The Regulation is applicable as of 1 July 2016, until when the Commission Decision 2009/767/EC [i.2], as amended, remains applicable. For trust services not covered by the Regulation, Member States remain free to define other types of trust services, for national purposes where these can be considered as qualified trust services (without effect in other Member States).

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 a given 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 need to 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 at a given time. Trusted lists therefore contain not only the service's current status, but also the history of its statuses.

The present document provides specifications for trusted lists in two contexts, namely the European Union legislative context as set by Regulation (EU) No 910/2014 [i.10] and the context of countries outside the European Union and the EEA countries, or of international organizations willing to 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 can be used to enable in practice any interested party to determine whether a trust service from a non-EU country or an international organization is or was operating under an approval scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place.

- 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.

NOTE 3: In order to validate that a trust service is a qualified one under Regulation (EU) No 910/2014 [i.10], a relying party would need to check the qualified status of the given trust service and that it is provided by a qualified trust service provider. Provided a trust service is included in the trusted list, it provides the relying party with the necessary information about the given trust service, its status and status history and potentially additional relevant information helping the relying party to validate the trust service or its outputs (e.g. certificate, signature or seal, time-stamp).

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 national 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/or sealed by its MS scheme operator and the certificate to be used to verify such a signature/seal 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 or seal 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.

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, their type 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 Regulation (EU) No 910/2014 [i.10] and in its applicable secondary legislation as of 1 July 2016.

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 digital signatures.

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

2 References

2.1 Normative references

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

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 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

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

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

[5] ISO/IEC 10646:2014: "Information technology - Universal Coded Character Set (UCS)".

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

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

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

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

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

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

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

[13] ISO/IEC 6429:1992: "Information technology - Control functions for coded character sets".

[14] ISO/IEC 2022:1994: "Information technology - Character code structure and extension techniques".

[15] ISO 3166-1:2013: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".

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

2.2 Informative references

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

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

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

[i.1] 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.

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

[i.5] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[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] ISO/IEC 17000:2004: "Conformity assessment - Vocabulary and general principles".

[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".

[i.10] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.11] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[i.12] ISO/IEC 9594-8:2014: "Information technology - Open System Interconnection - The Directory: Public-key and attribute certificate frameworks".

3 Definitions and abbreviations

3.1 Definitions

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

advanced electronic signature under e-signature Directive : advanced electronic signature as defined in Directive 1999/93/EC [i.3]

advanced electronic seal: As defined in Regulation (EU) No 910/2014 [i.10].

advanced electronic signature: As defined in Regulation (EU) No 910/2014 [i.10].

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: authority trusted by one or more users to create and assign certificates

NOTE 1: A certification authority can be:

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

(2) a technical certificate generation service that is used by a certification service provider that creates and assign public key certificates.

NOTE 2: See ISO/IEC 9594-8 [i.12] and Recommendation ITU-T X.509 [1].

certification service provider: 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

NOTE: From Regulation (EC) No 765/2008 [i.4] and 2.1 of ISO/IEC 17000:2004 [i.8].

digital signature: data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

electronic seal: As defined in Regulation (EU) No 910/2014 [i.10].

electronic signature: As defined in Regulation (EU) No 910/2014 [i.10].

(EU) qualified certificate: qualified certificate as specified in Regulation (EU) No 910/2014 [i.10]

qualified certificate under e-signature Directive: 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 seal: As defined in Regulation (EU) No 910/2014 [i.10].

qualified electronic signature: As defined in Regulation (EU) No 910/2014 [i.10].

qualified electronic signature/seal creation device: As defined in Regulation (EU) No 910/2014 [i.10].

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: signature-creation device, as defined in Article 2.5 of Directive 1999/93/EC [i.3], which meets the requirements laid down in annex III of [i.3]

signer: entity being the creator of a signature

signatory: As defined in in Regulation (EU) No 910/2014 [i.10].

seal creator: As defined in in Regulation (EU) No 910/2014 [i.10].

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

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

NOTE: Such trust services are typically but not necessarily using cryptographic techniques or involving confidential material.

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

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

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

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

NOTE: In the context of European Union Member States, as specified in Regulation (EU) No 910/2014 [i.10], it refers to a EU Member State list including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

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.

(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

3.2 Abbreviations

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

ACA	Attribute Certification Authority
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	Certification 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	Greece (ISO 3166-1 [15] Alpha 2 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
QSCD	Qualified Signature/Seal Creation Device
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
TSA	Time-Stamping Authority
TSL	Trust-service Status List
TSP	Trust Service Provider
TST	Time-Stamp Token
UCS	Universal Character Set
UK	United Kingdom (ISO 3166-1 [15] Alpha 2 country code for Great-Britain)
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
UTF	Unicode Transformation Format
WWW	World Wide Web
XAdES	XML Advanced Electronic Signature

NOTE As defined in ETSI TS 101 903 [3].

XHTML	eXtended HTML
XML	eXtensible Markup Language
EDS	Electronic Delivery Service

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.
   - 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.
   - (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.