ETSI TS 119 431-1 V1.1.1 (2018-12)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev

Reference
DTS/ESI-0019431-1

Keywords
e-commerce, electronic signature, remote,
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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

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

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

The present document is part 1 of a multi-part deliverable covering policy and security requirements for Trust Service Providers providing remote signature, as identified below:

Part 1: "TSP service components operating a remote QSCD / SCDev";

Part 2: "TSP service components supporting AdES digital signature creation".

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.

Executive summary

The present document specifies policy and security requirements for TSP service components operating a digital signature creation device, including a QSCD (Qualified Signature/Seal Creation Device) as defined in Regulation (EU) No 910/2014 [i.1] to create a digital signature value on behalf of a remote signer.

These requirements are based on the general policy requirements specified in ETSI EN 319 401 [1] and take into account related requirements for certificate issuance in ETSI EN 319 411-1 [2].

The requirements of the present document are aligned with the requirements specified in CEN EN 419 241-1 [3].

Introduction

When digital signatures are created in an entirely user-managed environment, it is assumed that the signature creation data is under the control of the signer, who is physically in possession of the signature creation device.

For remote digital signature creation, the signature creation data is maintained and managed by a third party on behalf of the signer. To guarantee that the signature creation environment is reliable and that the signature creation data is used under the control of the signer, the provider of the remote digital signature service has to apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels.

1 Scope

The present document specifies generally applicable policy and security requirements for Trust Service Providers (TSP) implementing a service component operating a remote signature creation device (SCDev). Specific requirements apply when the device is a QSCD as defined in Regulation (EU) No 910/2014 [i.1].

The service component consists of a signing application and a QSCD / SCDev. The term used in the present document is server signing application service component (SSASC).

The policy and security requirements are defined in terms of requirements for creation, maintenance, life-cycle management and use of signing keys used to create digital signatures.

The present document gives no restrictions on the type of TSP implementing such a component.

The present document is aimed to be used by independent bodies as the basis for a conformity assessment that a TSP can be trusted for operating a remote QSCD / SCDev.

The present document supports European and other regulatory frameworks.

NOTE 1: Specifically, but not exclusively, the present document is aimed at qualified and non-qualified trust service providers, providing the creation of digital signatures supporting electronic signatures and electronic seals (both advanced and qualified) in accordance with the requirements of Regulation (EU) No 910/2014 [i.1]. Annex A contains requirements that are specific for an SSASC in the context of Regulation (EU) No 910/2014 [i.1].

The present document does neither specify how fulfilment of the requirements can be assessed by an independent conformity assessment body, nor requirements for information to be made available to such independent assessors, or requirements on such assessors.

NOTE 2: See ETSI EN 319 403 [i.3] for guidance on assessment of a TSP's processes and services.

NOTE 3: The present document references ETSI EN 319 401 [1] for general policy requirements common to all TSP services covered by ETSI standards.

The present document does not specify protocols used to access the SSASC.

NOTE 4: Protocols for remote digital signature creation are defined in ETSI TS 119 432 [i.4].

The present document identifies specific controls needed to address risks associated with services operating remote QSCD / SCDev.

2 References

2.1 Normative references

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

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

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

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

[1] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

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

[3] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements".

2.2 Informative references

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

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

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

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.3] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.4] ETSI TS 119 432: "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

[i.5] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.6] ISO/IEC 15408: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.7] ISO/IEC 18014-2: "Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens".

[i.8] CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing".

[i.9] CEN 419 221-5: " Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services".

[i.10] ETSI 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

3 Definition of terms, abbreviations and notations

3.1 Terms

For the purposes of the present document, the terms given ETSI TR 119 001 [i.2] and the following apply:

NOTE: Where a definition is copied from a referenced document this is indicated by inclusion of the reference identifier number at the end of the definition.

authentication: provision of assurance in the claimed identity of an entity

NOTE: As defined in ISO/IEC 18014-2 [i.7].

digital signature value: result of the cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

electronic identification (eID): process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person

NOTE: As defined in Regulation (EU) No 910/2014 [i.1].

electronic identification means: material and/or immaterial unit containing person identification data and which is used for authentication for an online service

NOTE: As defined in Regulation (EU) No 910/2014 [i.1].

electronic identification means reference: data used in the SSASC as a reference to an electronic identification means in order to authenticate the signer

EXAMPLE: When the eID means uses asymmetric keys, the public key can be the reference.

When a signed assertion is generated after a successful authentication of the signer, the assertion signer id and the user id can be the reference.

When the eID means uses a secret key (e.g. one time password generator) the secret key can be the reference.

person identification data: set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established

NOTE: As defined in Regulation (EU) No 910/2014 [i.1].

qualified electronic signature/seal creation device (QSCD): as specified in Regulation (EU) No 910/2014 [i.1]

remote signature creation device: signature creation device used remotely from signer perspective and provides control of signing operation on the signer's behalf

server signing application service component (SSASC): TSP service component employing a server signing application to create a digital signature value on behalf of a signer

server signing application service provider (SSASP): TSP operating a server signing application service component

signature creation device (SCDev): configured software or hardware used to implement the signature creation data and to create a digital signature value

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

trust service provider (TSP): entity which provides one or more trust services

3.2 Abbreviations

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

eID	electronic IDentification
EUSCP	EU SSASC Policy
LSCP	Lightweight SSASC Policy
NCP	Normalized Certificate Policy
NSCP	Normalized SSASC Policy
OID	Object IDentifier
QSCD	Qualified electronic Signature/Seal Creation Device
SCDev	Signature Creation Device
SCP	SSASC Policy
SSASC	Server Signing Application Service Component
SSASP	Server Signing Application Service Provider
TSP	Trust Service Provider

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any SSASC policies. Such requirements are indicated by clauses without any additional marking;

b) requirements applicable under certain conditions. Such requirements are indicated by clauses marked by "[CONDITIONAL]";

c) requirements that include several choices which ought to be selected according to the applicable situation. Such requirements are indicated by clauses marked by "[CHOICE]";

d) requirements applicable to the services offered under the applicable SSASC policy. Such requirements are indicated by clauses marked by the applicable SSASC policy as follows:

"[LSCP]", "[NSCP]" and "[EUSCP]".

The requirements in the present document are identified as follows:

<3 letters service component> - < the clause number> - <2 digit number - incremental>

The SSASC service sub-components are:

- **OVR:** General requirement (requirement applicable to more than 1 service component)
- **GEN:** Signing Key Generation Service
- **LNK:** Certificate/eID means Linking Service
- **SIG:** Signature Activation Service
- **DEL:** Signing Key Deletion Service
- **EID:** eID Means Provision (optional)

The management of the requirement identifiers throughout subsequent editions of the present document is as follows:

- When a requirement is inserted at the end of a clause, the 2 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish a new requirement.
- The requirement identifier for deleted requirements are left and completed with "VOID".
- The requirement identifier for modified requirement are left void and the modified requirement is identified by capital letter(s) appended to the initial requirement number.

4 General concepts

4.1 General policy requirements concepts

The present document is structured broadly in line with ETSI EN 319 411-1 [2] to assist TSPs in applying these requirements to their own policy and practice statement documentation.

The present document incorporates CEN EN 419 241-1 [3] requirements by reference. CEN EN 419 241-1 [3] defines levels of assurance for sole control. The term "sole control" does not mean that the requirements are only applicable to electronic signatures as defined in Regulation (EU) No 910/2014 [i.1]. The requirements may be applied mutatis mutandis to electronic seals. In other words, the reader may replace the term "sole control" with "control" as explained in CEN EN 419 241-1 [3] clause 5.3.