ETSI TS 119 441 V1.1.1 (2018-08)

Electronic Signatures and Infrastructures (ESI);
Policy requirements for TSP providing signature validation services

Reference

DTS/ESI-0019441

Keywords

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
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

Contents

Intellectual Property Rights 5
Foreword....5
Modal verbs terminology....5
Introduction 5
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references....8
3 Definitions, abbreviations and notation....9
3.1 Definitions....9
3.2 Abbreviations 11
3.3 Notation....12
4 General concepts 12
4.1 General policy requirements concepts....12
4.2 Signature Validation Service applicable documentation 13
4.2.1 Signature Validation Service Practice Statements 13
4.2.2 Signature Validation Service Policy 13
4.2.3 Terms and conditions....13
4.2.4 Other documents associated with signature validation 14
4.3 Signature Validation Service components....14
4.3.1 Signature Validation Service actors....14
4.3.2 Architecture 15
4.3.3 Process....16
5 Risk assessment....18
6 Policies and practices 18
6.1 Signature Validation Service practice statement 18
6.2 Terms and Conditions 18
6.3 Information security policy 20
7 Signature Validation Service management and operation....20
7.1 Internal organization....20
7.2 Human resources 20
7.3 Asset management....20
7.4 Access control 20
7.5 Cryptographic controls 20
7.6 Physical and environmental security 21
7.7 Operation security 21
7.8 Network security 21
7.9 Incident management 21
7.10 Collection of evidence....22
7.11 Business continuity management 22
7.12 Signature Validation Service provisioning termination and termination plans 22
7.13 Compliance and legal requirements 22
8 Signature validation service technical requirements 23
8.1 Signature validation process....23
8.2 Signature validation protocol 24
8.3 Interfaces 24
8.3.1 Communication channel 24
8.4 Signature validation report 25
9 Framework for definition of validation service policies built on the present document....26
Annex A (informative): Table of contents for signature validation service practice statements 27

Annex B (normative): Qualified Validation Service for QES as defined by article 33 the Regulation (EU) No 910/2014.....29

Annex C (informative): Mapping of requirements to Regulation (EU) No 910/2014.....31

Annex D (informative): Recommendations on user interface 34

Annex E (informative): Checklist 35

Annex F (informative): Validation of validation report signature 36

History 37

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).

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

Digital signatures are a major cornerstone for electronic transactions, provided they can be validated in such a way that participants have confidence in the fact that they answer their (business) needs. In this perspective, a participant may call a Trust Service Provider (TSP) that will perform the validation of a digital signature on his behalf. Such TSP is called a Signature Validation Service Provider (SVSP). The outcome of such service is a (or a series of) signature validation report(s).

Participants of electronic transactions need to have confidence that the TSP has properly established procedures and protective measures in order to minimize the operational and financial threats and risks associated with digital signatures.

The present document is aiming to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, generally applicable requirements from Regulation (EU) No 910/2014 [i.1] that establishes a legal framework for electronic signature and electronic seal, including their validation.

Regulation (EU) No 910/2014 [i.1] defines Qualified Validation Service for qualified electronic signatures or for qualified electronic seals, a special type of signature validation service. Annex B provides additional requirements for EU qualified SVSPs (QSVSP) aiming to fulfil the requirements for qualified validation service for qualified electronic signatures or for qualified electronic seals as specified by Article 33 of Regulation (EU) No 910/2014 [i.1]. Bodies wishing to establish policy requirements for signature validation service providers in a regulatory context other than the EU can build their specifications on the present policy requirements to benefit from global best practices, and specify any additional requirements in a manner similar to the annex B.

1 Scope

The present document, based on the general policy requirements specified in ETSI EN 319 401 [2], specifies policy and security requirements for signature validation services operated by a TSP.

NOTE 1: Beside signature validation, other signature services, like signature creation, signature augmentation or signature preservation can also be offered by TSPs. Such services can be provided as stand-alone services or combined (e.g. augmentation can be used to support a preservation service). The present document does not provide requirements on signature services beyond validation and does not provide requirements on how to combine signature related services.

NOTE 2: A distinct Technical Specification (TS) provides policy and security requirements for TSP offering signature augmentation services as a stand-alone service or in complement to one of the above-mentioned services.

The present document is aimed at trust services supporting the validation of digital signatures in accordance with ETSI TS 119 102-1 [3]. It takes into account the relevant requirements for signature validation application specified in ETSI TS 119 101 [1] as they relate to TSPs.

It is aimed at supporting the validation of digital signatures in European and other regulatory frameworks.

NOTE 3: Specifically, but not exclusively, the present document is aimed at qualified and non-qualified trust services, supporting the validation of digital signatures in accordance with the requirements of the Regulation (EU) No 910/2014 [i.1] for validation of electronic signatures and electronic seals (both advanced and qualified). Annex B complements the requirements for signature validation service providers offering a Qualified Validation Service for qualified electronic signatures or for qualified electronic seals as specified by Regulation (EU) No 910/2014 [i.1].

NOTE 4: Specifically, but not exclusively, digital signatures in the present document cover electronic signatures, advanced electronic signatures, qualified electronic signatures, electronic seals, advanced electronic seals, and qualified electronic seals as per Regulation (EU) No 910/2014 [i.1].

The present document may be used by competent bodies as the basis for confirming that an organization is trustworthy in validating digital signatures on behalf of other persons or on its own behalf.

NOTE 5: See ETSI EN 319 403 [i.13] for guidance on assessment of TSP processes and services.

The user's interface is outside the scope of the main TSP service. However, the present document provides in annex D recommendations for the user's interfaces (for inputting the request and to visualize the validation report).

The TSP has connections with external (trust) services that can be contacted for provisioning validation information, or to relay the validation request. The present document does not put requirements on the trust service policies applied by such external services.

The present document identifies specific controls needed to address specific risks associated with validation services.

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 TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

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

[3] ETSI TS 119 102-1 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[4] ISO/IEC 15408 part 1 to 3: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[5] ISO/IEC 19790: "Information technology -- Security techniques -- Security requirements for cryptographic modules".

[6] FIPS PUB 140-2: "Security Requirements for Cryptographic Modules".

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 TS 119 102-2: "Elecrtonic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".

[i.4] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.5] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.6] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.7] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.8] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.9] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.10] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents".

[i.11] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists".

[i.12] ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services".

[i.13] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.14] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[i.15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.16] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[i.17] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[i.18] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".

[i.19] ETSI TS 119 172-2: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies".

[i.20] ETSI TS 119 172-3: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 3: ASN.1 format for signature policies".

[i.21] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

3 Definitions, abbreviations and notation

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI EN 319 401 [2], in ETSI TR 119 001 [i.2] and the following apply:

applicability checking: determination whether a signature conform to signature applicability rules

NOTE 1: The applicability checking is a broader concept than validation as covered by the present document: it is out of scope of the present document.

NOTE 2: The applicability checking can be provided as an adjunct to the signature validation service defined in the present document.

(signature) commitment type: signer-accepted indication of the exact implication of a digital signature

(signature) creation constraint: criteria used when creating a digital signature

driving application: application that uses a signature creation system to create a signature or a signature validation application in order to validate digital signatures or a signature augmentation application to augment digital signatures

NOTE: In a signature validation process, the driving application (DA) provides AdES digital signature and other input to a signature validation application (SVA).

qualified validation service for qualified electronic seals: As specified in Regulation (EU) No 910/2014 [i.1], Article 40.

qualified validation service for qualified electronic signatures: As specified in Regulation (EU) No 910/2014 [i.1], Article 33.

qualified validation service provider: SVSP that provides qualified validation service for qualified electronic seals or qualified validation service for qualified electronic signatures

signature acceptance: technical verification to be performed on the signature itself or on the attributes of the signature (i.e. the "signature elements constraints")

NOTE: The signature acceptance is a technical process defined and specified in ETSI TS 119 102-1 [3] and performed by a **signature validation application** (it is thus one part of the signature validation process). This signature validation application can be managed by a SVSP or can be a stand-alone application on the relying party environment.

signature applicability rules: set of rules, applicable to one or more digital signatures, that defines the requirements for determination of whether a signature is fit for a particular business or legal purpose

NOTE 1: Signature applicability rules can be implicit, or can be stated in a human readable document and/or in a machine processable from. ETSI TS 119 172-1 [i.10] can be used for this purpose.

NOTE 2: Rules in general can be any elements used by a user to decide whether a signature is fit for purpose (e.g. requirements on the time of signing, on the signer identity, on qualified signatures and statements, on use the validation report, etc.).

NOTE 3: Applicability rules can include for example:

- one or more signature validation policies containing validation constraints to be checked by the signature validation application,
- signature validation constraints or rules to be checked in addition to the checks carried out by the signature validation application.

NOTE 4: The owner of the signature applicability rules is usually the relying party and these rules can be shared by a community. Signature applicability rules can be handled by an extension to the service provided by the SVSP that would offer applicability checking and this is out of scope of the present document.

signature class: set of signatures achieving a given functionality

EXAMPLE: Signature with time, signature with long term validation material, Signature providing Long Term Availability and Integrity of Validation Material are possible signature classes.

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

signature validation application: application that validates a signature against a signature validation policy, and that outputs a status indication (i.e. the signature validation status) and a signature validation report

NOTE: The signature validation application (SVA) is specified in ETSI TS 119 102-1 [3].

signature validation client: component or piece of software that implements the signature validation protocol on the user's side

signature validation policy: set of signature validation constraints processed or to be processed by the SVA

NOTE 1: A signature validation policy is a purely technical concept. It is one of the inputs of a validation process (other inputs include the signed data and the signature) that determine the validation result (PASSED, FAILED or INDETERMINED).

NOTE 2: A signature validation policy can be imposed by signature applicability rules.

signature validation presentation: optional element in the signature validation process that can be used by a verifier to check the results of a validation process

signature validation report: comprehensive report of the validation provided by the signature validation application to the DA and allowing the driving application and any party beyond the driving application, to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the signature validation application

EXAMPLE: Clause 5.1.3 of ETSI TS 119 102-1 [3] specifies minimum requirements for the content of such a report and ETSI TS 119 102-2 [i.3] specifies such a report.

Signature Validation Service (SVS) policy: set of rules that indicates the applicability of a signature validation service to a particular community and/or class of application with common security requirements

NOTE: A SVS policy is applicable to a service; it is a specific sub-class of trust service policy as defined in ETSI EN 319 401 [2]. It relates to the quality and applicability of the service.

s**ignature validation service (SVS) practice statement:** statement of the practices and procedures used to address all the requirements identified for the provision of the signature validation service

NOTE: A signature validation service practice statement is a trust service practice statement that is part of the SVSP's documentation (see ETSI EN 319 401 [2]).

signature validation service server: component that implements the signature validation protocol and processes the signature validation on the SVSP's side

signature validation status: one of the following indications: TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE

signature validation: process of verifying and confirming that a digital signature is technically valid

signature verification: process of checking the cryptographic value of a signature using signature verification data

signer: entity being the creator of a digital signature

signature validation constraint: technical criteria against which a digital signature can be validated, e.g. as specified in ETSI TS 119 102-1 [3]

EXAMPLE: Criteria can be expressed as an abstract formulation of rule, value, parameter, range and computation result.

NOTE: Validation constraints can be defined in a formal signature validation policy, can be given in configuration parameter files or implied by the behaviour of the signature validation application.

user: application or human being interacting with an application on top of a signature validation client

validation: process of verifying and confirming that a certificate or a digital signature is valid

validation data: data that is used to validate a digital signature

validation of qualified electronic signature: As specified in Regulation (EU) No 910/2014 [i.1], Article 32.

validation of qualified electronic seals: As specified in Regulation (EU) No 910/2014 [i.1], Article 40.

validation service: system accessible via a communication network, which validates a digital signature

verifier: entity that wants to validate or verify a digital signature

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [2], in ETSI TR 119 001 [i.2] and the following apply:

DA	Driving Application
OVR	OVeRall
PoE	Proof of Existence
QES	Qualified Electronic Signature or Qualified Electronic Seal
(Q)SCD	(Qualified) Signature Creation Device
QSVSP	Qualified Signature Validation Service Provider
SD	Signer's Document
SDO	Signed Data Object
SDR	Signed Document Representation
SVA	Signature Validation Application