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

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).

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

SVP	Signature Validation Protocol
SVR	Signature Validation Report
SVS	Signature Validation Service
SVSP	Signature Validation Service Provider
SVSServ	Signature Validation Service Server
TSA	Time Stamping Authority
TSP	Trust Service Provider
VPR	signature Validation PRocess

3.3 Notation

The requirements identified in the present document include:

a) requirements applicable to any TSP conforming to the present document. 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]".

The requirements in the present document are identified as follows:

<the 3 letters identifying the elements of services > - < the clause number> - <2 digit number - incremental>

The elements of services are:

- **OVR:** General requirement (requirement applicable to more than 1 component)
- **SVP:** Signature validation protocol

NOTE: Specific protocol requirements are defined in ETSI TS 119 442 [i.12], the present document only provides policy requirements regarding protocol applicable to the service.

- **VPR:** Signature validation process
- **SVR:** Signature validation report

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

- When a requirement is inserted at the end of a clause, the 2 digits 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 new requirements.
- 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 in line with ETSI EN 319 401 [2]. It incorporates ETSI EN 319 401 [2] requirements by reference and adds requirements relevant for a SVSP.

See ETSI EN 319 401 [2], clause 4 for guidance on general policy requirements.

4.2 Signature Validation Service applicable documentation

4.2.1 Signature Validation Service Practice Statements

The SVSP develops, implements, enforces, and updates a **SVS practice statements** which is a trust service practice statement such as defined in ETSI EN 319 401 [2], instantiated for a signature validation service. See clause 6.1.

The SVS practice statements describe ***how*** the SVSP operates its service and is owned by the SVSP. The recipients of the practice statements can be the auditors, the subscribers and the relying parties.

NOTE: The presence of some elements is mandatory in the SVS practice statement as requested in the present document, however the present document places no restriction on the form of the SVS practice statement; it can be included in a general TSP practice statement document that covers other services delivered by that TSP or a standalone document. Annex A provides a recommended table of content.

The present document provides requirements identified as necessary to support a high-level signature validation service policy, to be endorsed by a SVSP and reflected in its **practice statements**.

4.2.2 Signature Validation Service Policy

A **SVS policy** describes ***what*** is offered and can contain diverse information beyond the scope of the present document to indicate the applicability of the service. The recipients of the service policy can be the subscribers and the relying parties.

The present document can be referred by such SVS policy to provide information about the level of the service.

SVSPs conforming to the present document's normative requirements except those from annex B may use in its documentation the following specific OID:

- itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) main (1)

QSVSP conforming to the present document's normative requirements including those defined in annex B may use in its documentation the following specific OID:

- itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) qualified (2)

According to ETSI EN 319 401 [2] it is mandatory for a TSP to identify the service policies it supports. For validation services, such identifier is communicated by the SVSP via the validation responses and/or reports and through the documentation provided to the subscribers and relying parties.

A SVS policy is not necessarily part of the SVSP's documentation (as per ETSI EN 319 401 [2] a practice statement and general terms and conditions are sufficient); e.g. a SVS policy can be shared by a community and not owned by the SVSP. Also, the present document does not put constraints on the form of the SVS policies; a SVS can be a stand-alone document or be provided as part of the practice statements and/or the general terms and conditions.

The present document does not put any limitation on the content of the SVS policies but it is requested that the SVSP provides minimal information about the service it offers (see clauses 6.1 and 6.2).

4.2.3 Terms and conditions

In addition to the SVS practice statements and, when issued by the SVSP, the signature validation service policy, the SVSP also issues **terms and conditions**, see clause 6.2. The terms and conditions are specific to a SVSP. The recipients of the terms and conditions can be the subscribers and the relying parties.

NOTE: The presence of some elements is mandatory in the terms and conditions as requested in the present document, however the present document places no restriction on the form of terms and conditions; it can be a standalone document for a public audience, or it can be split over subscriber's agreement(s) and information to relying parties. The form and content of the terms and conditions can also depend on national regulations.

4.2.4 Other documents associated with signature validation

The SVA works on the basis of a **signature validation policy** as input, i.e. a signature validation is always done against a signature validation policy. Such signature validation policy, which is the set of signature validation constraints processed or to be processed by the SVA, can be issued as a human readable document or machine processable. It can be identified by means of an OID/URI (see clause 8). The SVS can accept several sources of signature validation policies, including from the user.

Beyond the criteria against which signatures are technically validated, it is important to be able to determine if a signature is fitting a certain business need. **Signature applicability rules** can be used for this purpose. They can be structured as per ETSI TS 119 172-1 [i.10] and can include a signature validation policy containing the validation constraints to be checked by the SVA, as well as other criteria to be checked beyond the validation process. Going beyond the scope of a signature validation policy, the signature applicability rules *state the rules and assumptions* used by a *user* to decide whether a signature is *fit for purpose* and is usually owned by the relying party.

NOTE: The use of signature applicability rules is outside the scope of the present document but can be applied as an extension to the validation service as covered by the present document.

4.3 Signature Validation Service components

4.3.1 Signature Validation Service actors

The two main actors are the **SVSP**, which is a **Trust Service Provider** (**TSP**) and its **subscriber**. A SVSP can offer one or more signature validation services. Within a subscriber's umbrella, **user(s)** request signature validation.

NOTE: A signature validation service can be combined with a signature augmentation service. The protocol specified in ETSI TS 119 442 [i.12] supports the request for augmentation with validation.

A user is an application or a human being interacting with an application on top of the signature validation client (see clause 4.3.2). The requirements in the present document apply to the SVSP, neither to the user nor to the other actors that can be involved in the provision of signature validation services. Such other actors are listed below to give a complete picture of the validation landscape, they include:

- The signer can constrain/limit the signature (e.g. by means of a signature (creation) policy, a commitment type) and this can influence the signature validation
- The signer's related TSPs:
  - The TSP having issued the signer's certificate (CA);
  - Any TSP that can be implied in the signature generation:
    - the TSP handling the (Q)SCD on behalf of the signer;
    - the TSP generating the signature;
    - TSAs;
    - etc.
- Other TSPs:
  - TSAs;
  - other SVSPs to whom the SVSP can relay a request;
  - etc.
- The European or foreign trusted list providers; and
- The European Commission providing the List of Trusted Lists.

4.3.2 Architecture

The validation services are broken down into the following components:

- The signature validation client is a component or a piece of software that implements the signature validation protocol on the user's side. In particular it:
  - Requests a signature validation to the signature validation service server (SVSServ);

NOTE 1: It is possible to request the validation of multiple signatures (see ETSI TS 119 442 [i.12]). However, the present document and ETSI TS 119 442 [i.12] do not specify how to handle the relationships between multiple signatures, nor how to validate more complex structures such as ASiC.

  - Executes the signature validation protocol (SVP) on the user's side;
  - When applicable, cares for the validation report presentation;
  - The client can incorporate:
    - A user interface for manually inputting the request.
    - A machine interface for automated requests.
    - A user interface to present the report.

NOTE 2: The **applicability checking**, i.e. the final decision to "accept" a signature on the basis of the validation report (e.g. according to the reported cause(s) of an indetermination or specific information on the signature mentioned in the report), can be done by the user (manually), or the client, or the server (depending on the SVS implementation). This can be done according to **signatures applicability rules** such are specified in ETSI TS 119 172-1 [i.10].

- The signature validation service server (SVSServ) which is the component that implements the signature validation protocol on the SVSP's side. In particular it:
  - Executes the signature validation service protocol and processes the signature validation on the SVSP side;
  - Runs the signature validation application (SVA) such as defined in ETSI TS 119 102-1 [3], that implements the validation algorithm also defined in ETSI TS 119 102-1 [3]. For this purpose, the service can call external actors e.g. (non-exhaustive list):
    - The CA having issued the signer's certificate (for certificate(s) status information services (OCSP), or repository services to get a CRL).
    - The CA of the TSA(s) that have provided timestamps within the signature.
    - Other SVSP for complementary checks.
    - The European Member States trusted lists, the List of Trusted Lists of the European Commission, and/or other trusted lists.
    - etc.
  - Creates the signature validation report(s) related to the request;
  - Builds the signature validation response.

NOTE 3: As specified in ETSI TS 119 102-1 [3], the SVSServ implements the **SVA**, i.e. the application that implements the format checker, the identification of signer's certificate, the validation context initialization, the X.509 validation, the crypto validation, the signature acceptance (i.e. signature elements validation), and in option "other elements" validation).

NOTE 4: In the case of a validation service, the Driving Application (**DA**) can be fully on the client side or shared over client and server (e.g. the signature validation service server can implement part of the DA, e.g. to perform some applicability check). The present document does not put requirements on the client; only the DA's elements implemented on the server side are subject to requirements.

4.3.3 Process

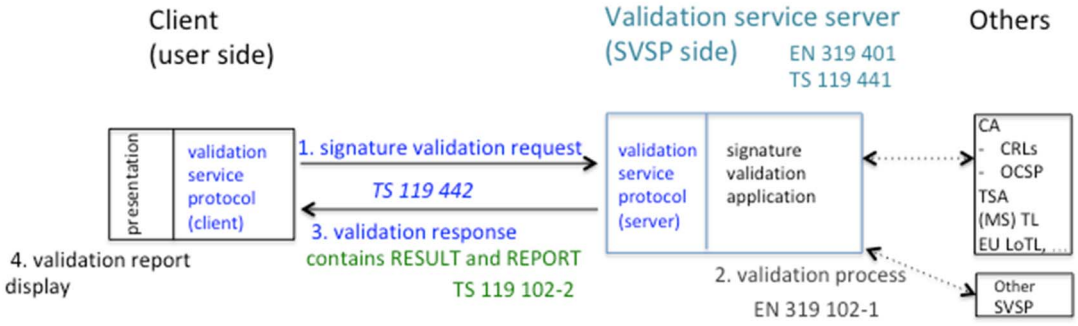

Figure 1: Validation process

The **communication channel** between the client and the SVSServ transports the signature validation request (1.) and the response (3.). It can be synchronous or asynchronous. It covers the authentication of the SVSP, to avoid false reports, and it can support client authentication.

The communication channel between the SVSP and other TSPs is out of scope of the present document (because most of the TSPs contacted by the SVSP, like the signer's related TSPs, are imposed). However, when the SVSP has the possibility to call a TSP of its choice to request some material (e.g. a timestamp) it has some responsibilities on the trustworthiness of such material (e.g. the called TSP is qualified, the information is signed by the called TSP, and/or the called TSP can be correctly authenticated).

Step 1. The client generates and submits a signature validation request.

The **protocols** supporting the request and response are specified in ETSI TS 119 442 [i.12].

The request includes:

1) The signed document(s) (SD) and the signature(s) (SDO(s)) that sign them; or

2) The signed document(s) representation(s) (SDR(s)) and the signatures that sign them, to avoid exposing document content to the validation service.

NOTE 1: The mapping between the signed documents(s) and their digests used within the signature(s) is essential when verifying a signature. For example in Regulation (EU) No 910/2014 [i.1] the link between the signed document and the signature is part of the conditions for an advanced electronic signature/seal. However due to confidentiality or performance reasons there are use cases where it is preferable to submit only the digests of the signed documents. In this case, where the client or a proxy computes the digest of the signed document(s), the verification of the signed document falls out of the control and responsibility of the SVSP.

3) (optional) Validation constraints, as defined in ETSI TS 119 102-1 [3]. Validation constraints can be inputted:

   a) Freely in the request as a machine processable signature validation policy or signature validation policy identifier that is to be used as a request for using the identified policy.

   b) Via an out-of-band process (for example a user interface proposed by the SVS).

NOTE 2: The present document does not require that a SVSP supports signature validation policies provided by the user. When this option is offered, the SVSP will not necessarily be able to always process the signature validation policy completely either:

- because it does not understand all or part of it, e.g. because it is not correctly formatted,
- it understands but has no tool/access to validate some elements, or
- because it conflicts with the SVSP practices (that may impose certain constraints to be checked in place or on top of the ones provided by the user).

Clause 8.1 provides requirements relating to how to consider validation policy provided by the user and how to manage possible conflicting sources of constraints.

NOTE 3: There are plans to define machine readable/processable signature validation policies (ETSI TS 119 172-2 [i.19] and ETSI TS 119 172-3 [i.20]).

NOTE 4: The validation process is agnostic with regard to the signed data. Certificates or timestamps can be submitted to the validation service and the algorithm specified in ETSI TS 119 102-1 [3] can perfectly be used for validating certificates or timestamps. However, such peculiar signed data are usually used for specific purposes where their validation is optimized according to the context of use. This tailoring is out of scope of the present document. The present document considers the validation of certificates and time stamps as components of the signature to be validated as specified in ETSI TS 119 102-1 [3].

Step 2. The SVSServ performs the validation process.

The **validation process** is specified in ETSI TS 119 102-1 [3].

Validation is carried out by the SVSP according to constraints that can be provided either by the client (1. in figure 1) and/or by the service itself:

1) If not provided by the client request, the SVS implements a "default value" signature validation policy.

2) If provided by the client, then the client signature validation policy can be completed as requested by the SVSP practices.

NOTE 5: ETSI TS 119 102-1 [3] provides a minimal set of validation constraints to consider for the signature validation process.

NOTE 6: This step implies requests to external services such as mentioned in clause 4.3.2.

Step 3. The SVSServ prepares and sends the validation response.

The **protocols** supporting the request and response are specified in **ETSI TS 119 442 [**i.12**]**.

The validation response embeds the validation report(s). It carries the OID of the service policy, and it can embed an OID of the signature validation policy used.

The **validation report** is specified in **ETSI TS 119 102-2 [**i.3**]**. It:

- Can be signed by the TSP.

NOTE 7: The present document does not put requirements on if this signature is done by a legal or natural person.

NOTE 8: Signing the report can be mandatory by regulatory frameworks.

NOTE 9: The signature on the report can be kept rather simple (e.g. a basic signature, see ETSI TS 119 102-1 [3]), see annex F for more details.

- Reports on each validation constraint:
  - when the constraint was processed, with the related result,
  - when the constraint was not processed with an indication that the constraint was ignored, or overridden, where relevant.

NOTE 10: See ETSI TS 119 102-1 [3] for guidance and ETSI TS 119 172-4 [i.11] for additional guidance for the EU qualified signature or seal case.

There is one validation report for each validated digital signature. Different levels of detail are possible (see ETSI TS 119 102-2 [i.3] for example). If a user wishes a global result this needs to be processed as part of the applicability checking that is out of scope of the validation process.

NOTE 11: When ETSI TS 119 102-2 [i.3] is followed, the different reports for multiple signatures that are validated within one requests (e.g. validation of one document with multiple signers), are signed together by the SVSP.

Step 4. **Validation report presentation**

The client can offer a signature validation presentation module to present the validation report and other relevant information (see clause 5.2.9 in ETSI TS 119 102-1 [3]).

Based on the validation report (e.g. reasons for "INDETERMINATE" status, or information provided in the report about the signed attributes), the user decides whether it accepts the signature on not.

EXAMPLE: The user can accept the signature or not based on the confirmed time of signature as part of applicability checking.

5 Risk assessment

OVR-5-01 The requirements specified in ETSI EN 319 401 [2], clause 5 shall apply.

6 Policies and practices

6.1 Signature Validation Service practice statement

OVR-6.1-01 The requirements specified in ETSI EN 319 401 [2], clause 6.1 shall apply.

In addition the following particular requirements apply:

OVR-6.1-02 The SVS practice statement should be structured as per annex A.

OVR-6.1-03 The SVS practice statement should list or make reference to (e.g. through OIDs), and briefly describe, the supported SVS policies.

OVR-6.1-04 The SVSP shall identify in the SVS practice statements the obligations of all external organizations supporting its services including the applicable policies and practices.

6.2 Terms and Conditions

OVR-6.2-01 The requirements specified in ETSI EN 319 401 [2], clause 6.2 shall apply.

NOTE 1: With regard to **REQ-6.2-02 k) in ETSI EN 319 401 [**2**]**; the SVSP can provide a notice that the SLA and also the signature validation status and the signature validation report can be affected by the practices, policies and SLAs of other TSPs, not under the control of the SVSP.

EXAMPLE 1: Depending on the certification practice statement corresponding to the signing certificate and the mechanism used to provide revocation status information, there can be a delay in disseminating revocation status information. Thus, the user may need to await the next CRL, or even one following that, to be assured any relevant revocation request has been processed.

NOTE 2: Unless specifically further detailed, the recipients of the terms and conditions are at least the subscribers and the relying parties.

In particular:

- **OVR-6.2-02** The terms and conditions shall list or make reference to (e.g. through OIDs), and briefly describe, the supported SVS policies.
- **OVR-6.2-03** To further specify the trust service policy being applied, the terms and conditions may refer to the OIDs defined in clause 4.2.2. to provide information about the level of the service.

In addition the following particular requirements apply:

OVR-6.2-04 The referred SVS policies shall be available to the subscriber.

In particular:

- **OVR-6.2-05 [CONDITIONAL]** If the SVS policy is not a document owned by the SVSP, it shall be publicly available.
- **OVR-6.2-06 [CONDITIONAL]** If the SVS policy is not a stand-alone document the terms and conditions shall clearly indicate which information the service policy OID refers to and where to find it.

EXAMPLE 2: The service policy can be defined as (elements of) the practice statements and/or of the terms and conditions and/or elements from public document such as the present document.

OVR-6.1-07 The terms and conditions or the referred SVS policy shall list or make reference to (e.g. through OIDs) the supported signature validation policies.

OVR-6.2-08 The terms and conditions or the referred SVS policy shall describe the options supported by the service. At least:

a) If the service allows the user to select:

   i) the Signed Data Object (SDO) to verify and the Signer's Document (SD) to verify if it is not included in the SDO,

   ii) the certificate(s) to be used for the validation, e.g. for the case where attributes of the SDO do not contain the certificate(s) needed,

   iii) the specific signature to be verified in the case the SDO contains multiple signatures, and

   iv) the implicit or explicit signature validation policy to be used amongst the available ones.

b) If the service allows the user to provide further inputs for the validation process (i.e. elements to parameterize the validation policy such as the signature class, a trust anchor, etc.);

c) The signature formats it supports.

EXAMPLE 3: Formats specified in ETSI EN 319 122-1 [i.4] and ETSI EN 319 122-2 [i.5] or in ETSI EN 319 132-1 [i.6] and ETSI EN 319 132-2 [i.7] or in ETSI EN 319 142-1 [i.8] and ETSI EN 319 142-2 [i.9].

OVR-6.2-09 The terms and conditions or the referred SVS policy shall document how the service will handle the validation of signatures with expired or obsolete elements (e.g. expired certificates or timestamps, revoked certificates, usage period of cryptographic algorithms exceeded).

NOTE 3: Guidance on cryptographic algorithms validity can be found in ETSI TS 119 312 [i.14].

NOTE 4: This information can be given by referencing the corresponding validation algorithm (e.g. ETSI TS 119 102-1 [3]).

OVR-6.2-10 [CONDITIONAL] When the service allows the client to provide or to select signature validation policy information, the terms and conditions or the referred SVS policy shall describe the behaviour of the signature validation process.

In particular:

a) how the SVS selects the validation constraints when conflicting indication is provided by the client (e.g. indication in a specific validation constraints provided by the client conflicting with the SVSP's practice/policies),

b) how the SVSP sets the validation constraints when the signature validation policy provided by the client is not complete enough,

c) how the SVSP handles the case where it is not possible to process the constraints submitted by the client, e.g. it is not able to interpret them or it has no right to access required evidence, etc.,

d) under which conditions the signature validation policy provided by the user can be ignored and replaced by a SVSP signature validation policy.

NOTE 5: The protocol specified in ETSI TS 119 442 [i.12] supports diverse possibilities.

OVR-6.2-11 The terms and conditions or the referred SVS policy shall clearly state what is considered as PoE of the signature.

OVR-6.2-12 The terms and conditions shall either indicate the rights and obligations, or disclaim any responsibility on the activities, of the actors listed in clause 4.3.1.

OVR-6.2-13 [CONDITIONAL] When the client is allowed to take a role in the validation (e.g. calculating the hash), the terms and conditions shall describe under which conditions this can be done, and precise in particular if there are limitations in the responsibility taken be the SVSP.

OVR-6.2-14 SVSP shall state which algorithm it applies in its documentation available to relying parties (i.e. the practice statements if they are public, or the terms and conditions or the referred SVS policy).

EXAMPLE 4: ETSI TS 119 102-1 [3].

6.3 Information security policy

OVR-6.3-01 The requirements specified in ETSI EN 319 401 [2], clause 6.3 shall apply.

In addition the following particular requirements apply:

OVR-6.3-02 The security policy should document the security and privacy controls implemented to protect personal data.

NOTE: If the SVSP has access to signed data this can contain personal data.

7 Signature Validation Service management and operation

7.1 Internal organization

OVR-7.1-01 The requirements specified in ETSI EN 319 401 [2], clause 7.1 shall apply.

7.2 Human resources

OVR-7.2-01 The requirements specified in ETSI EN 319 401 [2], clause 7.2 shall apply.

7.3 Asset management

OVR-7.3-01 The requirements specified in ETSI EN 319 401 [2], clause 7.3 shall apply.

7.4 Access control

OVR-7.4-01 The requirements specified in ETSI EN 319 401 [2], clause 7.4 shall apply.

7.5 Cryptographic controls

OVR-7.5-01 The requirements specified in ETSI EN 319 401 [2], clause 7.5 shall apply.

In addition, the following particular requirements apply:

OVR-7.5-02 [CONDITIONAL] When validation reports are signed the SVSP should select a signing certificate issued by a trustworthy CA that implements ETSI EN 319 411-1 [i.16] or ETSI EN 319 411-2 [i.17].

OVR-7.5-03 [CONDITIONAL] When validation reports are signed, the SVSP private signing key shall be held and used within a cryptographic module which:

a) Is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [4], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or

b) Meets the requirements identified in ISO/IEC 19790 [5] or FIPS PUB 140-2 [6], level 3.

OVR-7.5-04 [CONDITIONAL] When validation reports are signed, the secure cryptographic device required by **OVR-7.5-03** should be as per **OVR-7.5-03 a)**.

OVR-7.5-05 [CONDITIONAL] When validation reports are signed, any backup copies of the SVSP private signing keys shall be protected to ensure its integrity and confidentiality by the cryptographic module before being stored outside that device.

7.6 Physical and environmental security

OVR-7.6-01 The requirements specified in ETSI EN 319 401 [2], clause 7.6 shall apply.

In addition the following particular requirement apply:

OVR-7.6-02 The following requirement specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SVA: **GSM 1.4**.

7.7 Operation security

OVR-7.7-01 The requirements specified in ETSI EN 319 401 [2], clause 7.7 shall apply.

In addition the following particular requirements apply:

OVR-7.7-02 The following requirements specified in ETSI TS 119 101 [1], clause 5.2 should apply to the SVA: **GSM 1.2**.

OVR-7.7-03 The following requirements specified in ETSI TS 119 101 [1], clause 5.2 should apply to the SVA: **GSM 1.3**.

OVR-7.7-04 The following requirements specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SVA: **GSM 2.4**.

7.8 Network security

OVR-7.8-01 The requirements specified in ETSI EN 319 401 [2], clause 7.8 shall apply.

In addition the following particular requirements apply:

OVR-7.8-02 In case remote access to systems storing or processing confidential data is allowed, a formal policy should be adopted, and described as part of elements required by **OVR-6.3-02**.

OVR-7.8-03 In case remote access to systems storing or processing confidential data is allowed, appropriate security measures shall be implemented to protect against the risks of remote access.

NOTE: This confidential information can be subscriber related info (like preferences), or signed data that would be stored waiting further processing (e.g. if revocation status data is unavailable).

7.9 Incident management

OVR-7.9-01 The requirements specified in ETSI EN 319 401 [2], clause 7.9 shall apply.

7.10 Collection of evidence

OVR-7.10-01 The requirements specified in ETSI EN 319 401 [2], clause 7.10 shall apply.

In addition the following particular requirements apply:

OVR-7.10-02 The SVSP shall implement event logs to capture information needed for later proofs.

In particular:

- **OVR-7.10-03** Any signature validation shall be logged, possibly together with the identification of the subscriber when this information is known.

NOTE: To log the identity of a subscriber is a business decision of the TSP. GDPR [i.15] requires a clear purpose to do so.

- **OVR-7.10-04** Event logs shall be marked with the time of the event.

OVR-7.10-05 The frequency of processing, the (maximal) retention periods, the protection, the back-up procedures of the collection system, the archiving procedures and the vulnerability assessment of the event logs shall be documented in the SVS practice statement.

OVR-7.10-06 The implementation of requirements OVR-7.10.1 to OVR-7.10.3 shall take the applicable privacy requirements into account.

OVR-7.10-07 Event logs should include the type of the event, the event success or failure, and an identifier of the person and/or component at the origin for such an event.

7.11 Business continuity management

OVR-7.11-01 The requirements specified in ETSI EN 319 401 [2], clause 7.11 shall apply.

In addition in order to provide business continuity as specified in the terms and conditions the following particular requirements apply:

OVR-7.11-02 Best reasonable efforts shall be undertaken to keep the service available in line with the Service-Level Agreement (SLA), and the necessary technical and organizational precautions shall be taken to ensure this alignment (e.g. is there a business continuity plan, a disaster recovery plan in place, etc.).

OVR-7.11-03 Measures should be implemented to avoid interruption by third parties or unintentional interruptions by the user.

OVR-7.11-04 [CONDITIONAL] When validation reports are digitally signed and expected to be validated over the long term, the SVSP should select a signing certificate issued by a CA that provides guarantees on the availability of the information on the status of its certificates and that has a termination plan clearly described in its CPS.

NOTE: CA that conforms to ETSI EN 319 411-1 [i.16] or ETSI EN 319 411-2 [i.17] implements recognized best practices.

OVR-7.11-05 [CONDITIONAL] When validation reports are digitally signed and expected to be validated over the long term, the SVSP should select trusted source(s) for proofs of existence (e.g. a qualified time stamping authority).

7.12 Signature Validation Service provisioning termination and termination plans

OVR-7.12-01 The requirements specified in ETSI EN 319 401 [2], clause 7.12 shall apply.

7.13 Compliance and legal requirements

OVR-7.13-01 The requirements specified in ETSI EN 319 401 [2], clause 7.13 shall apply.

In addition the following particular requirements apply:

OVR-7.13-02 When personal data is processed by a third party an appropriate agreement shall be made with third party processors of personal data in order to ensure that they do comply with the requirements stated in the SVSP practice statements and terms and conditions, including with regard to the implementation of technical, organizational and legal measures to protect the personal data.

NOTE 1: Both the signed data and the signature may contain personal data.

OVR-7.13-03 The SVSP shall NOT store the SD after processing when not necessary.

NOTE 2: If the validation service works in combination of a preservation service such data may need to be kept.

OVR-7.13-04 the SVSP shall have the overall responsibility for meeting the requirements defined in clauses 5 to 8 even when some or all of its functionalities are undertaken by sub-contractors.

8 Signature validation service technical requirements

8.1 Signature validation process

VPR-8.1-01 The validation process shall comply with ETSI TS 119 102-1 [3].

NOTE 1: This does not mean that the SVSP has to implement the algorithm specified in ETSI TS 119 102-1 [3], as it allows alternative implementations provided that they produce the same main status indication when given the same set of input information.

In particular:

- **VPR-8.1-02** The minimal set of constraints requested by clause 5.1.4.1 of ETSI TS 119 102-1 [3] may be further specified, e.g. as per ETSI TS 119 172-1 [i.10] (e.g. a list of accepted commitment types).

NOTE 2: The signature validation policy is not limited in size or number of constraints (see ETSI TS 119 102-1 [3]).

VPR-8.1-03 The validation process shall output a signature validation status indication, one per validated signature, and a signature validation report.

VPR-8.1-04 According to the algorithm specified in ETSI TS 119 102-1 [3], the signature validation status required in **VPR-8.1-03** shall be TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE.

VPR-8.1-05 The SVS shall support at least one (or more) signature validation policy(ies) in such a way that there is always one signature validation policy available as input to the SVA.

NOTE 3: A SVS may be unable to check all the constraints of a signature validation policy; the list of actually processed constraints including their result (e.g. PASSED, FAILED, INDETERMINATE) provided in the validation report represents the signature policy used. See also ETSI TS 119 102-2 [i.3].

VPR-8.1-06 The SVS may accept several sources of validation policy, including from the user.

VPR-8.1-07 The validation application (SVA) should comply with the requirements in ETSI TS 119 101 [1], clause 7.4 **SIA 1 to SIA 4**.

VPR-8.1-08 The validation process shall ensure that the signature validation policy that is used corresponds to the strategy defined in the SVS policy and/or the terms and conditions of use of the SVS.

VPR-8.1-09 The strategy defined in the SVS policy and/or the terms and conditions of use of the SVS for the selection of the signature validation policy shall at least follow the next principles:

- [CONDITIONAL] When the client inputs/selects a signature validation policy the SVSP should as far as possible use the signature validation policy requested by the client.
- [CONDITIONAL] When no signature validation policy is provided by the client the SVSP shall use (one of) its own signature validation policy(ies).

- [CONDITIONAL] When the signature validation policy provided by the client is not complete the SVSP shall complete it with validation constraint(s) in such a way that the minimal set of validation constraints imposed by the SVSP (as per practice statement or terms and conditions) is reached.

- [CONDITIONAL] When there is an indication in a specific validation constraint in the signature validation policy provided by the client conflicting with the SVSP's polices, the SVSP shall have a process to determine the precedence.

NOTE 4: Nothing obliges a SVSP to consider all the constraints from a signature validation policy requested by a client as validation constraints for the signature validating process. There are different cases: the SVSP can decide to impose its signature validation policy. A second case is when the SVSP tries to use the policy referred in the signature but is not able to process it completely (either because it does not understand all or part of it (too exotic or partly not correctly formatted), or because it understands but has no tool/access to validate some elements). ETSI TS 119 442 [i.12] supports error message in the case where the signature validation policy requested by the client cannot be processed; it also supports a way to convey the list of supported signature validation policies to the client.

VPR-8.1-10 [CONDITIONAL] When it is the SVSP that computes the hash of the SD or any attribute like archival attributes, it shall confirm that the integrity of the SD (resp. attribute) has not been compromised.

NOTE 5: When it is the client that computes hash(es) this cannot be ensured by the SVSP and left to the responsibility of the client (see also **OVR 6.2-16**). In particular, the expected hash(es) are the ones computed with the same hash functions than the ones used in the signature.

VPR-8.1-11 [CONDITIONAL] When the SVS aims to validate qualified electronic signatures or qualified electronic seals such as defined by Article 32.1 (reps. 40) of the Regulation (EU) No 910/2014 [i.1], validation process should follow the requirements of ETSI TS 119 172-4 [i.11].

VPR-8.1-12 For the same input, the signature validation service shall also have the same output.

NOTE 6: The signature validation policy used is part of the input (independent from its source).

VPR-8.1-13 The SVS may accept different elements as proofs of existence of a signature.

EXAMPLE: External inputs or inputs taken from the signature (self-claims, time-stamps, etc.)

8.2 Signature validation protocol

SVP-8.2-01 The protocol used by the SVSP should conform to ETSI TS 119 442 [i.12].

SVP-8.2-02 [CONDITIONAL] When the SVS provides the option to receive a detailed report and/or to receive the validation status in the response, then the SVS shall ensure consistency between the status provided in the report and in the response.

SVP-8.2-03 The signature validation response should bear the OID of the SVS policy.

8.3 Interfaces

8.3.1 Communication channel

SVP-8.3.1-01 The communication channel between the client and the SVSP shall be secured; i.e. the SVSP shall offer a way to be authenticated by the client and the confidentiality of the data shall be ensured.

SVP-8.3.1-02 The SVSP may securely authenticate the client.

NOTE: The identification of the client is especially important if (s)he takes a role in the validation (calculating the hash). In particular, when only the hash is provided to the SVSP, this is a risk for the human end-user. If he receives the validation report via an intermediate that operates the validation client, the validation client could maliciously present a wrong report to the end-user, by providing a wrong hash to the SVS (e.g. deliver hash and signature of another validly signed document to the SVSP and deliver the report on that to the end-user for a malicious document). This authentication is important for traceability reasons.

8.4 Signature validation report

SVR-8.4-01 The SVS shall output a status indication and a validation report providing the details of the technical validation of each of the applicable constraints (see ETSI TS 119 102-1 [3]).

SVR-8.4-02 The validation report should conform to ETSI TS 119 102-2 [i.3].

SVR-8.4-03 The signature validation report shall indicate one of the three status defined in ETSI TS 119 102-1 [3], i.e. TOTAL-PASSED, TOTAL-FAILED or INDERTERMINATE.

SVR-8.4-04 The validation report shall report sub-indications as specified in ETSI TS 119 102-1 [3].

SVR-8.4-05 The signature validation report shall report on each of the validation constraints that is processed including any validation constraints that have been applied implicitly by the implementation.

SVR-8.4-06 [CONDITIONAL] When the SVS is able to validate signatures against a well identified signature validation policy, the signature validation report may bear the identifier of the signature validation policy.

NOTE 1: This is done consistently with the strategy described in the SVSP documentation (**see OVR-6.2-10**).

NOTE 2: This identifier is present in the validation response when the protocol conforms to ETSI TS 119 442 [i.12] and is present in the validation report when it conforms to ETSI TS 119 102-2 [i.3].

EXAMPLE: The referred signature validation policy can be present whether it was completely processed or not, with or without additional validation constraints, or it can only be present when it was completely processed with no additional constraints, etc.

SVR-8.4-07 [CONDITIONAL] When a signature validation policy is not completely processed by the SVS, the report in addition to reporting on validated constraints, should report on constraints that have been ignored or overridden.

SVR-8.4-08 The signature validation report shall bear the identity of the SVSP.

SVR-8.4-09 [CONDITIONAL] When ETSI TS 119 102-2 [i.3] is followed, the signature validation report shall bear the "Validator Information" as defined in ETSI TS 119 102-2 [i.3].

NOTE 3: In the case of a signature validation service, the validator is the SVSP.

SVR-8.4-10 The signature validation report shall report the signer's identity.

SVR-8.4-11 The signature validation report shall report on any signed attributes (e.g. commitment type).

NOTE 4: In case of a non-critical signed attribute, that cannot be decoded, it might be sufficient to put just information on that the attribute is there.

SVR-8.4-12 The signature validation report shall bear signature validation process information (e.g. such as defined in ETSI TS 119 102-2 [i.3]) with the following element:

a) An identifier indicating the validation process (see ETSI TS 119 102-1 [3] , clauses 5.3, 5.5 and 5.6.3) that has been used in validation.

SVR-8.4-13 [CONDITIONAL] When timestamps are present, the validation report should report on the quality of the timestamps (e.g. EU qualified or not).

SVR-8.4-14 The validation report shall clearly indicate if the SVS did not perform the hash computation but relied on such a computation done by the client.

SVR-8.4-15 The validation report should clearly indicate the origin of each PoE (from within the signature, from the client, from the server).

SVR-8.4-16 The validation report should bear a validation report signature and this should be the SVSP's digital signature.

SVR-8.4-17 [CONDITIONAL] When validation reports are signed the format and the target of the signature should conform to ETSI TS 119 102-2 [i.3].

SVR-8.4-18 [CONDITIONAL] When validation reports are signed the signature may be in a basic form; it does not need to be time-stamped or further augmented. See also annex F.

SVR-8.4-19 [CONDITIONAL] When the validation report is presented through a webpage the SVSP shall be authenticated within a TLS session.

9 Framework for definition of validation service policies built on the present document

OVR-9-01 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; the policy shall incorporate, or further constrain, all the requirements identified in clauses 5 to 8.

OVR-9-02 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; the policy shall identify any variances it chooses to apply.

OVR-9-03 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; subscribers shall be informed, as part of implementing the terms and conditions, of the ways in which the specific policy adds to or further constrains the requirements of the policy as defined in the present document.

OVR-9-04 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; there shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the policy.

OVR-9-05 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; a risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the policy for the stated community and applicability.

OVR-9-06 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; the policy should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the policy.

OVR-9-07 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; a defined review process should exist to ensure that the policy is supported by the practices statements.

OVR-9-08 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; the TSP should make available the policies supported by the TSP to its user community.

OVR-9-09 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; revisions to policies supported by the TSP should be made available to subscribers.

OVR-9-10 [CONDITIONAL] When building a validation service policy built on requirements defined in the present document; a unique object identifier shall be obtained for the policy (e.g. OID or URI).

Annex A (informative): Table of contents for signature validation service practice statements

1. Introduction

1.1 Overview

1.1.1 TSP identification

1.1.2 Supported signature validation service policy(ies)

(*formal OID/URI identification)*

1.2 Signature Validation Service Components

1.2.1 SVS actors

1.2.3 Service architecture

1.3 Definitions and abbreviations

1.3.1 Definitions

1.3.2 Abbreviations

1.4 Policies and practices

(this clause is about the TSP documentation and the service backgrounds i.e. risks assessment, Inf.Sec. Pol.)

1.4.1 Organization administrating the TSP documentation

1.4.2 Contact person

1.4.3 TSP (public) documentation applicability

This clause describes the set of documents related to the validation services, their applicability, and position of the present practice statement within the documentation, their distribution points …

At a minimum the following documents exist and need a short description:

- *the present practice statement (formal OID/URI identification should be used);*
- *the terms and conditions;*
- *the service policy (can be referred)*

one or more of the above documents identify the supported signature validation polic(ies) (with formal OID/URI identification). The supported signature validation polic(ies) are generally detailed in the signature validations service polic(ies)

- *risk assessment and Information security policy*

NOTE: The description of any business (application) domain or any transactional context described in a "signature applicability rules" document. There is no obligation for a TSP to support and publish such rules.

2. Trust Service management and operation

*This clause may be common to any services offered by the TSP - except for CA that should follow the IETF RFC 3647's ToC [*i.21*].*

(Either the same clause is reproduced for each service practice statements, in which case because each service policy and security requirements adds elements specific to the services, such requirements need to be addressed in addition, OR there is a common clause that is referred to from each service practice statements).

2.1 Internal organization

2.1.1 Organization reliability

(This clause identifies the obligations of all external organizations supporting the TSP services including the applicable policies and practices (per ETSI EN 319 401 [2])

2.1.2 Segregation of duties

2.2 Human resources

2.3 Asset management

2.3.1 General requirements

2.3.2 Media handling

2.4 Access control

2.5 Cryptographic controls

2.6 Physical and environmental security

2.7 Operation security

2.8 Network security

2.9 Incident management

2.10 Collection of evidence

2.11 Business continuity management

2.12 TSP termination and termination plans

2.13 Compliance

3. Signature validation service design

3.1 Signature validation process requirements

This clause contains requirements, control objectives and controls in connection with clause 8.1 in ETSI TS 119 441.

3.2 Signature validation protocol requirements

3.3 Interfaces

This clause contains requirements, control objectives and controls in connection with clause 8.3 in ETSI TS 119 441.

3.3.1 Communication channel

3.3.2 SVSP - other TSP

3.4 Signature validation report requirements

This clause contains requirements, control objectives and controls in connection with clause 8.4 in ETSI TS 119 441.

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

VPR-B-01 [CONDITIONAL] If the SVSP is a QSVSP, all the requirements from clauses 5 to 9 shall apply.

In addition:

VPR-B-02 [CONDITIONAL] If the SVSP is a QSVSP the implementation should comply with ETSI TS 119 172-4 [i.11].

NOTE 1: When the signature is not fully conformant to the requirements of a Qualified Electronic Signature /Seal, the SVSP can provide complementary information about the signature or seal, e.g. if it is an advanced electronic signature/seal based on a EU qualified certificate.

NOTE 2: This recommendation will be replaced by a normative provision when ETSI TS 119 172-4 [i.11] is published.

OVR-B-03 [CONDITIONAL] If the SVSP is a QSVSP, the SVSP shall test its service to demonstrate the correct implementation of **VPR-B-02** and shall describe such tests in its practice statements.

OVR-B-04 [CONDITIONAL] If the SVSP is a QSVSP, the tests in **OVR-B-03** should check different use-cases, positive and negative ones.

SVR-B-05 [CONDITIONAL] If the SVSP is a QSVSP, the validation report shall bear the digital signature of the SVSP.

SVR-B-06 [CONDITIONAL] If the SVSP is a QSVSP, the validation report shall be provided to the client in an automated manner that can be processed by a machine.

NOTE 3: Complying with ETSI TS 119 442 [i.12] and with ETSI TS 119 102-2 [i.3] will allow to satisfy this requirement.

SVR-B-07 [CONDITIONAL] If the SVSP is a QSVSP, when the validation report is presented through a webpage the SVSP should be authenticated within a TLS session supported by a certificate issued by a certification authority operating under ETSI EN 319 411-2 [i.17] and conforming to ETSI EN 319 412-4 [i.18].

SVR-B-08 [CONDITIONAL] If the SVSP is a QSVSP, when timestamps are present, the validation report shall report if the timestamp is a qualified electronic time-stamp as per Regulation (EU) No 910/2014 [i.1].

SVR-B-09 [CONDITIONAL] If the SVSP is a QSVSP, the information requested by **SVR-8.4-08 and 09** shall be under the form of a certificate that bears the name of the QSVSP such as indicated in the official status.

OVR-B-10 [CONDITIONAL] When the QSVSP conforms to all normative requirements of the present document including those specified in the present annex B, the QSVSP may use the specific service policy OID defined in clause 4.2.2.

VPR-B-11 [CONDITIONAL] If the SVSP is a QSVSP, the SVSP should control the hash computation (either perform the computation on the server side or control the client if it is allowed on the client side).

NOTE 4: Regulation (EU) No 910/2014 [i.1] specifies that the link between the signed document and the signature is part of the conditions for an advanced electronic signature/seal (Article 26 & 36). Article 32 explicitly requires that the validation process validate such conditions.

VPR-B-12 [CONDITIONAL] If the SVSP is a QSVSP, the signature validation policy shall clearly be identified as a validation policy for validating that a signature is a qualified electronic signature or seal as per Regulation (EU) No 910/2014 [i.1].

NOTE 5: ETSI TS 119 172-4 [i.11] will have an OID for identifying such a signature validation policy.

SVR-B-13 [CONDITIONAL] If the SVSP is a QSVSP, the validation report shall indicate whether the qualified electronic signature is an EU qualified electronic signature or an EU qualified electronic seal.

NOTE 6: ETSI TS 119 172-4 [i.11] allows to proactively report that an advanced electronic signature/seal is a QES.

VPR-B-14 [CONDITIONAL] If the SVSP is a QSVSP, the validation report shall allow the relying party to detect any security relevant issues.

VPR-B-15 [CONDITIONAL] If the SVSP is a QSVSP, in order to satisfy **VPR-B-13** to **VPR-B-14** the validation report should comply with ETSI TS 119 102-2 [i.3].

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

The qualified validation of QES is specified by Article 33.1 of the Regulation (EU) No 910/2014 [i.1] as follows:

"A qualified validation service for qualified electronic signatures ***may only be provided by a qualified trust service provider*** *who:*

a) provides validation in compliance with Article 32(1); and

b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service."

For the qualified validation of qualified electronic seal the Regulation (EU) No 910/2014 Article 40 [i.1] is applicable. Article 40 states that Articles 32 and 33 "*shall apply mutatis mutandis to the validation… of qualified electronic seals"*. Unless stated specifically, in the rest of the present annex QES will mean indifferently qualified electronic seal or qualified electronic signature.

Qualified trust service provider

The requirements for qualified trust service providers are provided in Article 24.2 (a) to (j) of Regulation (EU) No 910/2014 [i.1]. They are covered by the present document as follows.

Article 24.2 of Regulation (EU) No 910/2014 [i.1]	Requirements from present document
(a) inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;	(this is not specified by technical standards)
(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;	OVR-7.2-01 OVR-7.13-04
(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;	OVR-7.1-01
(d) before entering into a contractual relationship, inform, in a clear and comprehensive manner, any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;	Clause 6.2
(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them;	Clause 7.7, in particular OVR-7.7-01 Clause 8
(f) use trustworthy systems to store data provided to it, in a verifiable form so that: (i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained, (ii) only authorised persons can make entries and changes to the stored data, (iii) the data can be checked for authenticity;	 Clause 7.13 OVR-7.2-01 Clause 7.5
(g) take appropriate measures against forgery and theft of data;	Clauses 7.6 and 7.7

Article 24.2 of Regulation (EU) No 910/2014 [i.1]	Requirements from present document
(h) record and keep accessible for an appropriate period of time, including after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;	Clauses 7.10, 7.11
(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article 17(4);	Clause 7.12
(j) ensure lawful processing of personal data in accordance with Directive 95/46/EC.	Clause 7.13

Providing validation in compliance with Article 32(1)

The validation of QES as specified by the Regulation (EU) No 910/2014 [i.1] requires the verification of the conditions listed in Article 32.1 of the Regulation (EU) No 910/2014 [i.1].

To ensure that all conditions required by the Regulation (EU) No 910/2014 [i.1] Article 32.1 and 40 are verified, a correct validation algorithm is needed. It provides the same deterministic result for a signature or seal submitted to validation. The signature validation policy is crucial for this purpose. ETSI TS 119 172-4 [i.11], based on the validation algorithm specified in ETSI TS 119 102-1 [3] has been issued with this perspective.

The combination of the two above-mentioned standards allows to confirm **each element of Article 32.1 (reps. 40)** of the Regulation (EU) No 910/2014 [i.1]. This is covered by the present document as follows.

Article 32.1 of Regulation (EU) No 910/2014 [i.1]	Requirements from present document
Verification of the conditions listed in Article 32.1 of the Regulation (EU) No 910/2014	VPR-8.1-01, VPR-B-02, VPR-B-03

NOTE: The validation process for EU qualified electronic signature applies thus *mutatis mutandis* to the validation of EU qualified electronic seal, except the validation requirements relating to pseudonym that are not applicable to electronic seals. Also, the validation process for qualified electronic seal will ensure that the conditions of Article 36 are fulfilled (instead of Article 26). To this regard, the control on the seal creation data by the creator of the seal needs to be ensured, rather than the sole control.

The assessment of the conformity to the Regulation (EU) No 910/2014 [i.1] Article 32 and 40 will necessarily require to test the implementation with, e.g. a series of sample signatures and seal. The EC puts tools at disposal to do so (Connecting Europe Facility (CEF)). They can be used by the SVSP to demonstrate their service conformity and by any conformity assessment body or supervisory body. This is covered by **OVR-B-04 and OVR-B-04_bis.**

Allowing relying parties to receive the result of the validation process as requested in Article 33.1 (b)

The requirements with regard to the reception of the result of the validation process are covered by the present document as follows.

Article 33.1 (b) of Regulation (EU) No 910/2014 [i.1]	Requirements from present document
in an automated manner;	SVR-B-06
which is reliable; See note.	SVR-B-07, SVR-B-09, VPR-B-12 See also below
which is efficient;	SVR-B-06
bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.	SVR-B-05, OVR-7.5-02
NOTE: The reliability of the content is addressed below, in the consideration related to Article 32.2.	

Article 32.2 (resp. 40) - correct result and detection of security issues

In addition, although not specifically required for a qualified validations service, to ensure that the conditions required by the Regulation (EU) No 910/2014 [i.1] Article 32.2 and 40 are verified, the signature validation report is crucial.

ETSI TS 119 102-2 [i.3] has been issued with this perspective, and is recommended as per **SVR-8.4-01** and **VPR-B-16**. Regulation (EU) No 910/2014 [i.1] Article 32.2 and 40 are supported by the present document as follows.

Article 32.2/40 of Regulation (EU) No 910/2014 [i.1]	Requirements from present document
The system used for validating the qualified electronic signature shall provide correct result of the validation process	SVR-8.4-01, OVR-B-03, OVR-B-04, VPR-B-11
The system used for validating the qualified electronic signature shall allow the relying party to detect any security relevant issues	OVR 6.2-13, VR-B-08, VPR-B-15 (i.e. VPR-B-13, SVR-B-14)

Annex D (informative): Recommendations on user interface

The following recommendations are for the case that the user interface is part of the SVS.

E-01 [CONDITIONAL] If the user interface is part of the SVS, the user interface should provide the result of the verification in a clear way to the user.

E-02 [CONDITIONAL] If the user interface is part of the SVS, the user interface should be able to present, upon request from the user, a summary of the validation result to the user in a human readable form.

E-03 [CONDITIONAL] If the user interface is part of the SVS, the user interface should be able to display the validation report.

E-04 [CONDITIONAL] If the user interface is part of the SVS, the user interface should be able to present the purported signer's identity, including:

a) the signer's certificate subject's distinguished name;

b) any signed attributes;

c) the distinguished name of the issuing CA; and

d) the distinguished name of the hierarchically superior CAs.

E-05 [CONDITIONAL] If the user interface is part of the SVS, the user interface should be able to present:

a) the identifier of the signature validation policy used in the validation process;

b) any known commitment implied by the signature.

E-06 [CONDITIONAL] If the user interface is part of the SVS, the requirements specified in ETSI TS 119 101 [1], clause 5.1 should apply.

E-07 [CONDITIONAL] If the user interface is part of the SVS, the validation report should be displayed to the client in an 'efficient'/'user friendly'/'understandable' manner.

Annex E (informative): Checklist

This annex provides a checklist for self-assessment or independent conformity assessment of TSPs offering signature validation services according to ETSI TS 119 102-1 v1.2.1 [3] and ETSI TS 119 101 [1] where applicable.

It also aims to facilitate the preparatory activities the trust service provider undertakes.

In case of conflict between the requirements listed in the checklist and those specified in the referenced documents, the referenced documents take precedence.

The checklist is in the file "Annex-to-TS_119441_v111.xlsx" contained in archive ts_119441v010101p0.zip which accompanies the present document and is available at https://www.etsi.org/deliver/etsi_ts/119400_119499/119441/01.01.01_60/.

Annex F (informative): Validation of validation report signature

The validation report can be digitally signed, and the user might ask if he has to use a validation service to validate the signature of the validation report, which would lead to a chicken-and-egg problem.

The value of a signature validation service is that the signatures which it is able to validate can be quite complex. The validation service is able to handle complicated scenarios, including the validation in archival format having several levels of archival attributes and handling a large variety of certificate paths to validate. In addition, the validation service can verify additional aspects, like checking if a signature is EU qualified, or if it contains a specific set of attributes.

On the other hand, the signature of the validation report has a very specific purpose. It guarantees the integrity and the origin of the report; it shows that the validation was done by a specific trust service provider and that it was not changed.

In general, to verify these two points it is not necessary to do a complex validation. It is sufficient to check the signing certificate and that the digital signature can be verified with the corresponding public key.

For example in the case of an EU qualified validation service, the signing certificate used in the report can be used to check the trustworthiness of the service by looking it up in the European trusted list. Similar checks on the trustworthiness can be done if a set of certificates of trusted services is available. If the signing certificate is directly contained in such a trust store, it is not even necessary to create the corresponding certificate path.

The validation resulting in a validation report and the one to verify the signature of the validation report are not of the same complexity and it is not needed to have a validation service to handle the second one, every basic signature validation tool is able to do this.

There may be use-cases where the information provided by a SVSP is to be used as evidence for the long-term preservation of the validated signature. In particular the validation report might need to be preserved; specific solutions avoiding the chicken-and-egg issue mentioned above are specified in signature preservation services documentation and are out of the scope of the present document.

History

Document history		
V1.1.1	August 2018	Publication