Draft ETSI TS 119 441 V0.0.4 (2017-11)

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

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 30 JANUARY 2018

Download the template for comments:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

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

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

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 commerce, 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 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 commerce 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. TSPs can use the service OID defined in this document to indicate that their services conform to the main part of the present document.

Annex C 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]. It provides requirements for service policies called « qualified », building on the present document. EU TSPs can use the specific service OID defined in the present document to indicate that their services conform to the present document and to the Annex C requirements aiming to fulfil the Regulation (EU) No 910/2014 [i.1] requirements. 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 C.

1 Scope

The present document, built on the general policy requirements specified in EN 319 401 [2], specifies policy and security requirements for signature validation services as well as signature validation with augmentation services operated by a trust service provider. This is aimed at trust services supporting the validation of digital signatures in accordance with EN 319 102-1 [i.3] . It takes into account the relevant requirements for signature validation application specified in ETSI TS 119 101 [1] as they relate to TSPs.

The present document aims at supporting the validation and optionally the augmentation of digital signatures in European and other regulatory frameworks.

NOTE 1: 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 C 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 2: 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]. Annex B provides specific requirements for the validation of qualified electronic seals or signature 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 and/or augmenting digital signatures on behalf of other persons or on its own behalf.

editorial note: may be make the link with EN 419 103 and assessment schemes

editorial note: would it be worth to provide a checklist, similar to the one provided with EN 319 411-1 /-2 in annex?

The user's interface is outside the scope of the main TSP service. However the present document provides in Annex E 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 policy applied by such external services.

This 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".

editor note: provided updating 119 101

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); definitions".

editor note: in waiting that the TR is updated to consider latest discussions in the STF and in ESI some concepts are slightly redefined in the present document.

[i.3] ETSI EN 319 102-1:"Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"

editor note: in waiting that the EN is updated to consider latest discussions in the STF and in ESI some concepts are slightly redefined in the present document.

[i.4] ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for creation and validation of AdES Digital Signatures. Part 2 - Signature Validation Report"

[i.5] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[i.6] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[i.7] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[i.8] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures".

[i.9] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[i.10] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[i.11] ETSI TS 119 172-1: "Electronic Signatures and Infrastructures (ESI); Building blocks and table of contents for human readable signature policy documents"

[i.12] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature applicability rules for European qualified electronic signatures/seals using trusted lists"

editor note: in waiting that the TS 119 172 part 1 and part 4 are updated to consider latest discussions in the STF and in ESI some concepts are slightly redefined in the present document.

[i.13] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"

[i.14] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles"

[i.15] ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol for TSPs providing signature validation services"

[i.16] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Editor note: some definitions in 119 001 (and other documents – 319 102-1, 119 101) need to be updated – in the meantime they are reproduced below

applicability checking: determination whether a signature is fit for a given business or legal purpose.

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

NOTE 2: The applicability checking may be provided as an adjunct the signature validation service defined in this standard.

NOTE 3: The applicability checking can be done by a human being or automated process, which is usually the relying party or its driving application.

NOTE 4: The applicability checking is to be done on top of a signature validation process, on the basis of the signature validation result and / or the information found in the validation report. For example, if the signer's identity found in the validation report is not the one expected by the relying party, the signature may be rejected.

Editorial note: was previously "conformance checking" in EN 319 102-1 conformance is a word to avoid as too regulatory oriented.

(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 signatures: as specified in Regulation (EU) No 910/2014 [i.1], Article 33

Qualified Validation Service for qualified electronic seals: as specified in Regulation (EU) No 910/2014 [i.1], Article 40

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: signature acceptance is technical process defined and specified in EN 319 102-1 [i.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.

Editorial note: this is called "signature acceptance validation" in 319 102-1. Signature acceptance is a subset of signature validation – it's a well-defined set of steps (in EN 319 102-1). It speaks by itself and does not need the word "validation"

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.11] 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 can they be shared by a community. Signature applicability rules can however 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.

Editorial note1: this was formerly called "signature validation policy": the term "signature validation policy" is now used for listing the technical constraints that are used to initiate a validation process (to be aligned with EN 319 102-1).

Editorial note2 "Signature applicability rules" concept may have a link with "signature creation policy" or not; the STF validation did not want to address the STF creation components, but the STF creation is informed that it needs to review applicable definitions, starting with creation policy.

"Signature applicability rules" currently has a link with « signature policy » but this concept also needs to be revised; in the same vein, the STF did not re-defined "signature policy" as it goes beyond the scope of the STF –this will be discussed at the steering or ESI level.

signature augmentation: process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term

NOTE: Augmenting signatures is a co-lateral process to the validation of signatures, namely the process by which certain material (e.g. time stamps, validation data and even archival-related material) is incorporated to the signatures for making them more resilient to change or for enlarging their longevity.

signature augmentation constraint: technical criteria used when augmenting a signature to a specific signature class

signature augmentation policy: set of signature augmentation constraints

NOTE: This covers collection of information and creation of new structures that allows performing, on the long term, validations of a signature.

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 application: application within the signature creation system, complementing the signature creation device, that creates a signature data object

signature creation data: unique data, such as codes or private cryptographic keys, which are used by the signer to create a digital signature value

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

signature creation environment: physical, geographical and computational environment of the signature creation system

signature creation system: overall system, consisting of the signature creation application and the signature creation device, that creates a digital signature

signature level: format specific definition of a set of data incorporated into a digital signature, which allows to implement a signature class

EXAMPLE: CAdES-B-B, CAdES-E-EPES [**Error! Reference source not found.**] and [**Error! Reference source not found.**], XAdES-B-LTA, XAdES-E-C [[i.7]] and [**Error! Reference source not found.**], PAdES-B-T, PAdES-E-LTV [[i.9]] and [**Error! Reference source not found.**] are examples of signature levels.

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

signature validation client: a component or a 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: SVA is defined in ETSI EN 319 102-1 [i.3]

NOTE 2: a signature validation policy is a purely technical concept. It is one of the inputs of a validation process (other inputs are a.o. the signed data and the signature) and it determines the validation result (PASSED, FAILED or INDETERMINED).

NOTE 3: the minimal set of constraints requested by ETSI EN 319 102-1 [i.3] can be further specified, e.g., as per ETSI TS 119 172-1 [i.11] (e.g. a list of accepted commitment types). The signature validation policy is not limited in size or number of constraints (see ETSI EN 319 102-1[i.3])

NOTE 4: a signature validation policy can be identified by an OID and a SVSP can identify the signature validation polic(ies) supported by its services by this means.

NOTE 5: a SVA always works on the basis of a signature validation policy as input. A SVSP needs to support one (or more) signature validation policy in such a way that there is always one signature validation policy available as input to the SVA.

NOTE 6: the SVSP can accept several sources of validation policy, including from the user.

NOTE 7: a SVS may be unable to check all the constraints of a signature validation policy; the list of actually processed constraints including their result (PASSED, FAILED, INDETERMINED) provided in the validation report represents the signature policy used. See also ETSI TS 119 102-2 [i.4].

NOTE 8: 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 SVA to the DA and allowing the DA and any party beyond the DA, to inspect details of the decisions made during validation and investigate the detailed causes for the status indication provided by the SVA

NOTE: clause 5.1.3 of ETSI EN 319 102-1 [i.3] specifies minimum requirements for the content of such a report and ETSI TS 119 102-2 [i.4] 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 1: 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. It relates to the quality and applicability of the service (controls in place, etc.).

NOTE 2 : a SVS policy may be specified in a document but this is not necessarily a stand-alone document that is part of the SVSP's documentation (see EN 319 401; a practice statement and general terms and conditions are sufficient). However, it is mandatory for a TSP to have or to refer to a service policy (EN 319 401). An OID can be used for this. This OID can mentioned in the practice statement and /or can be communicated by the TSP via the validation responses and/or reports.

Signature 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 EN 319 401).

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 device: configured software or hardware used to implement the signature verification data

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 EN 319 102-1 [i.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.

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

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

validation of qualified electronic seals: validation 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

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

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

3.2 Symbols

For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

Editorial note: to be completed if needed

3.3 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:

AES: Advanced electronic signature or advanced electronic seal
AES-QC: AES with qualified certificate
DA: Driving Application
OVR: overall
QC: qualified certificate
QES: qualified electronic signature or qualified electronic seal
SD: Signer's Document
SDO: Signed Data Object
SVA: Signature Validation Application

SVI: signature validation interface
SVP: Signature Validation Protocol
SVR: signature validation request
SVS: Signature Validation Service
SVSP: Signature Validation Service Provider
SVSServ: Signature Validation Service Server
TSA: Time Stamping Authority
VPR: Signature validation process

3.4 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 119 442 [i.15], the present document only provides policy requirements regarding protocol applicable to the service.
- **VPR**: Signature validation process
- **SVR**: Signature validation report
- **SVI**: Interfaces with related external services or client interface

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 digit number above is incremented to the next available digit.
- When a requirement is inserted between two existing requirements, capital letters appended to the previous requirement identifier are used to distinguish 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.

4.2 Signature Validation Service Practice Statements

4.2.1 Signature Validation Service applicable documentation

The present document constitutes a **signature validation service (SVS) policy** that serves as a basis for the SVSP to develop, implement, enforce, and update a **SVS practice statement** that covers all the requirements identified as necessary to provide a high level signature validation service.

NOTE 1: the presence of some elements is mandatory in TSP practice statement, 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.

In addition to the SVS practice statement the SVSP issues terms and conditions, see clause 6.2.

4.2.2 Signature Validation Service Policy

The present TS 119 441 is a specific instance of service policy as defined in ETSI EN 319 401 [2], it provides elements for a SVS implementing best practices.

SVSPs following the present document can claim conformance to the present document via the following specific trust service policy OID:

itu-t(0) identified-organization(4) etsi(0) VAL SERVICE-policies(9441) policy-identifiers(1) main (1)

Editorial note: OID to be confirmed

SVSP following the present document and providing qualified validation service (as specified in Annex C of the present document) can claim conformance to the present document via the following specific service policy OID:

itu-t(0) identified-organization(4) etsi(0) VAL SERVICE-policies(9441) policy-identifiers(1) qualified (2)

Editorial note: OID to be confirmed

NOTE : a SVSP can describe its service policy in a document and define it's own OID and / or refer the OIDs defined above in its practice statement or general terms and conditions.

4.2.3 Other documents associated with signature validation

Besides the description of the practices employed by the SVSP to offer the signature validation service, it is important to document the criteria against which signatures are validated and, beyond this, can than be determined as fitting a certain business need.

Two documents can be used for these purposes:

- A **signature validation policy** which is the set of **signature validation constraints** processed or to be processed by the SVA. A validation process is always done against a signature validation policy. A signature validation policy can be identified by means of an OID;
- **Signature applicability rules** that can be structured as per ETSI TS 119 172-1 [**Error! Reference source not found.**] 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.

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

The SVS practice statement, the signature validation policy and the signature applicability rules are different documents; the SVS practices statement describe ***how*** the SVSP operates its service, while the signature validation policy *states the constraints* to be processed by a *SVA* to decide whether a signature is *technically valid*. 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*.

The owner of the SVS practice statement is a SVSP, while the owner of the signature applicability rules is usually the relying party.

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 or validation with augmentation.

NOTE: There is always a signature validation before any signature augmentation.

A user can be a human being or 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 and neither the user nor on 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 as 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 or augmentation to the signature validation service server (SVSServ),
  - 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 1: 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 against **Signatures applicability rules** such are specified in ETSI TS 119 172-1 [i.11] . Specific applicability rules for QES provided in ETSI TS 119 172-4 [i.12].

- 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) and can run a signature augmentation application, such as defined in ETSI EN 319 102-1 [i.3], that implements the validation algorithm also defined in ETSI EN 319 102-1 [i.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 or information on the certificate applicability and level of assurance),

    - TSA(s) that have provided timestamps to the signer,

    - TSA(s) to provide (additional) timestamps for augmentation purposes,

    - Other SVSP for complementary checks,

    - The European Member States Trusted Lists and /or the List of the List of the European Commission.

    - etc…

  - augments the signature when this is requested,

  - creates the signature validation report(s) related to the request,

  - builds the signature validation or augmentation response.

    NOTE 2: As specified in ETSI EN 319 102-1 [i.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 3 The 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).

    NOTE 4: a signature augmentation application takes inputs from and provides the augmented signature to the DA.

4.3.3 Process

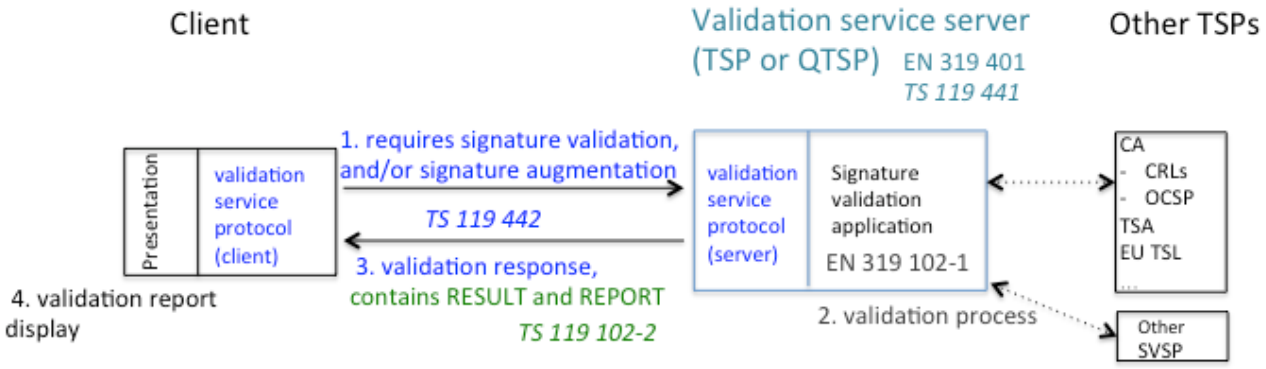

Figure 1 : Validation process.

The **communication channel** between the client and the SVSServ transports the signature validation (optionally with augmentation) request (1.) and the response (2.). It can be synchronous or asynchronous. It needs to cover 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, or, a signature validation with augmentation request.**

The **protocols** supporting the request and response are specified in ETSI TS 119 442 [i.15] .

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)) (or hash(es), or digests(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 EN 319 102-1 [i.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 policy provided by the user. When this option if 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 as it is not correctly formatted, or
- 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 and 119 172-3).

Step 2. The SVSServ performs the validation process.

The **validation process** is specified in ETSI EN 319 102-1 [i.3].

Validation is carried out by the SVSP according to constraints that can be provided either by the client (1. in figure **Error! Reference source not found.**) 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 client signature validation policy can be completed with signature validation constraints requested by the SVSP practices.

NOTE 4: ETSI EN 319 102-1 [i.3] provides a minimal set of validation constraints to consider for the signature validation process.

NOTE 5: 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.15].

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.4]. It:

- can be signed by the TSP

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

NOTE 9: The signed report can be long term ready (e.g. a signature providing long term availability and integrity of validation material, see ETSI EN 319 102-1 [i.3]).

- reports on each validation constraints:
    - 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 [i.3] and ETSI TS 119 172-4 [i.12] for guidance

There is one validation report for each validated digital signature. Different levels of detail are possible (see ETSI TS 119 102-2 [i.4]). 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.

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 EN 319 102-1 [i.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 with the "trust service policy" in ETSI EN 319 401 [2] referring to the level of service defined by the present document.

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 it conforms to. It may use the OIDs defined in clause 4.2.2 to do so.

OVR-6.1-04 The SVS practice statement or the terms and conditions shall list or make reference to (e.g. through OIDs) the supported signature validation policies.

OVR-6.1-05 The SVS practice statement or the terms and conditions shall document how the service will handle the validation of "old" signatures, where certificates may have expired or may have been revoked or even where the usage period of cryptographic algorithms may have been exceeded.

OVR-6.1-06 [CONDITIONAL] When the service allows the client to provide signature validation policy information, the SVS practice statement or the terms and conditions 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.

OVR-6.1-07 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 with the "trust service policy" in ETSI EN 319 401 [2] referring to the level of service defined by the present document.

In particular,

- **OVR-6.2-02** To specify the trust service policy being applied, the SVS terms and conditions shall list or make reference to (e.g. through OIDs), and briefly describe, the supported SVS Policies it conforms to.
- **OVR-6.2-03** To specify the trust service policy being applied, the SVS terms and conditions may use the OIDs defined in clause 4.2.2.

In addition the following particular requirements apply:

OVR-6.2-04 The terms and conditions shall indicate the rights and obligations of the actors listed in clause 4.3.1.

OVR-6.2-05 The terms and conditions 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 / augmentation policy such as the signature class, a trust anchor, etc.);

c) The signature formats it supports.

OVR-6.2-06 The terms and conditions shall include Service-Level Agreement (SLA) elements in the terms and conditions concerning that assured availability of the service and when applicable, other information on the reliability of the service such as response(s) time.

OVR-6.2-07 The terms and conditions shall provide a notice that the SLA and also the signature validation status and the signature validating report can be affected by the practices, policies and SLAs of other TSPs, not under the control of the SVSP.

EXAMPLE: Depending on 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.

Editorial note: probably need to work more on terms and conditions stating liabilities relating to external TSPs (TSAs, CAs and providers of revocation information.

OVR-6.2-08 The terms and conditions shall explain the personal data processing strategy of the SVSP.

Editorial note: this requirement is not "validation" specific. May be to consider in 319 401 for the future

OVR-6.2-09 [CONDITIONAL] when the supported signature validation policie(s) are not provided to through OVR-6.1-05 in the service practice statement (or if the service practice statement is not publicly available), they shall be listed or being referred to (e.g. through OIDs) in the terms and conditions.

OVR-6.1-10 [CONDITIONAL] if the information mentioned in OVR-6.1-06 is not provided in the service practice statement (or if the service practice statement is not publicly available), then it needs to be part of the terms and conditions.

OVR-6.1-11 [CONDITIONAL] if the information mentioned in OVR-6.1-07 is not provided in the service practice statement (or if the service practice statement is not publicly available), then it needs to be part of the terms and conditions.

OVR-6.2-12 [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.

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.

Editor note; if these data are considered as personal data from the subscribe, how would data privacy regulation apply?

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

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** and **GSM 1.3**.

OVR-7.7-03 The following requirements specified in ETSI TS 119 101 [1], clause 5.2 shall apply to the SVA: **GSM 2.4**.

Editorial note: these requirements could be generalised and not be "validation" specific.

OVR-7.7-04 The requirement specified in ETSI TS 119 101 [1], clause 5.3 shall apply.

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.

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 or augmentation shall be logged, together with the identification of the subscriber when this information is known.
- **OVR-7.10-04** event logs shall be marked with the time of the event.

OVR-7.10-05 The frequency of processing, the retention period, 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.
Editorial note: requirements 05 to 07 could be generalised, as they are not "validation" specific.

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 any interruption due to users or third parties (intentional or unintentional).

Editorial note : may be to be completed by specific measure to prevent DoS, unavailability of TSA, what to do when the CA does not respond, etc.

OVR-7.11-03 [CONDITIONAL] when validation reports are signed, in order to ensure that the validation reports can be validated over the long term, the SVSP should select a signing certificate issued by a CA that implements best practices, and in particular 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 or 411-2 implements recognised best practices.

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, if needed by the law, an appropriate agreement shall be made with third party processors of personal data in order to ensure that they do comply with the legal requirements, including the implementation of technical, organizational and legal measures to protect the personal data.

NOTE: this signed data is to be considered as personal data

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

NOTE: if the validation service works in combination of a preservation service such data will 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.

Editorial note: do we need to request that the TSP is a legal entity ? Actually this is not specific to validation services but there is nothing in ETSI EN 319 401 [2]on this topic.

8 Signature validation service

8.1 Signature validation process

VPR-8.1-01 The validation process shall comply with ETSI EN 319 102-1 [i.3] .

In particular:

- **VPR-8.1-02**: The validation process shall output a status indication, one per validated signature, (i.e. the signature validation status TOTAL-PASSED, TOTAL-FAILED or INDERTMINATE) and a signature validation report.

VPR-8.1-03 The validation application (SVA) should comply with the requirements in ETSI TS 119 101 [1] **clause 7.4 SAI 1 to SAI 4** and **SAI 9**.

VPR-8.1-04 The validation process shall ensure there is no code in the SD that would deceive the verifier (i.e. the user) as to what is seen is what is signed.

VPR-8.1-05 The validation process shall ensure that the signature validation policy that is used corresponds to the strategy defined in the practice statement and / or the terms and conditions of use of the SVS.

VPR-8.1-06 The strategy defined in the practice statement 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;
- [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 a indication in a specific validation constraints 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: 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).

SVR-8.1-07 [CONDITIONAL] When a signature validation policy requested by the client 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.

VPR-8.1-08 [CONDITIONAL] when it is SVSP that computes the hash of the SD, it shall confirm that the integrity of the signed data has not been compromised.

NOTE: when it is client that computes the hash this cannot be ensured by the SVSP and left to the responsibility of the client.

VPR-8.1-9 [CONDITIONAL] When the SVS aims to validate qualified electronic signatures or qualified electronic seals such as defined by the Regulation (EU) No 910/2014 [i.1], validation process shall follow the requirements listed in Annex B of the present document.

8.2 Signature augmentation process

VPR-8.2-01 The augmentation process shall comply with ETSI EN 319 102-1 [i.3] .

NOTE: it means a.o. that the minimal set of validation constraints defined in TS 119 102-1 [i.3] are to be processed

VPR-8.2-02 The SVSP shall insure that the timestamps used in augmentation process come from a TSA that follows state-of-the-art practices.

In particular

- **VPR-8.2-03** the TSA should conform to ETSI EN 319 421 [i.13] .

VPR-8.2-04 The SVSP shall insure that the timestamps used in augmentation process shall be as defined in IETF RFC 3161 [4] and updated by IETF RFC 5816 [9].

In particular

VPR-8.2-05 the timestamps used in augmentation process should be conform to ETSI EN 319 422 [i.14] .

VPR-8.2-06 The SVSP shall always perform a signature validation before any signature augmentation and shall include the validation result in the augmentation report.

VPR-8.2-07 The requirements defined in clause 8.3.5 in ETSI TS 119 101 [1] shall apply

8.3 Signature validation / augmentation protocol

SVP-8.3-01 The protocol used by the SVSP should conform to ETSI TS 119 442 [i.15].

SVP-8.3-02 [CONDITIONAL] When the SVS provide 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-8.3-03 the signature validation response shall bear the OID of the SVS policy.

8.4 Interfaces

8.4.1 Communication channel

SVP-8.4.1-01 The communication channel between the client and the SVSP shall be secured; i.e. the SVSP shall be authenticated by the client and the confidentiality of the data shall be ensured.

SVP-8.4.1-02 The client may be securely authenticated by the SVSP

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.

8.4.2 Signature Validation Service Provider – other Trust Service Providers

Editorial note: the validation protocol cares for the validation of information fetched @ CAs, TSA, etc. : do we want to add / further enforce these interfaces beyond what is stated in 6.2?

8.5 Signature validation report

SVR-8.5-01 The validation report should conform to ETSI TS 119 102-2 [i.4]

SVR-8.5-02 The signature validation report shall bear the Validator Information as defined in ETSI TS 119 102-2 [i.4].

SVR-8.5-03 The validation report should bear a validation report signature and this should be the AES signature of the SVSP.

SVR-8.5-04 [CONDITIONAL] when the validation report is presented through a webpage the SVSP shall be authenticated within a TLS session.

SVR-8.5-06 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-8.5-07 The signature validation report shall report the signer's identity

SVR-8.5-08 The signature validation report shall report on any signed attributes (e.g. commitment type).

SVR-8.5-09 The signature validation report may bear the signature validation policy identifier when a well-identified signature validation policy has been used with no additional validation constraints.

SVR-8.5-10 the signature validation report shall bear the following signature validation process information (e.g. such as defined in ETSI TS 119 102-2 [i.4]) with the following elements**:**

a) the identifier indicating the validation process (see ETSI EN 319 102-1 [i.3] , clauses 5.3, 5.5, 5.6.3) that has been used in validation;

b) the identifier of the validation service policy;

c) information identifying the validation service practice statement and / or the general term and conditions;

d) information on augmentation of the signature, when applicable;

Editorial note: c) is to indicate the way the constraints have been defined and/or the origin of the constraint (esp. in case of conflict or in the case of a signature validation policy provided by the client but incomplete, to indicate how the SVS has completed).

SVR-8.5-11 The validation report should report on the quality of the timestamps (e.g. qualified or not).

SVR-8.5-12 The validation report should clearly indicate when the SVS did not performed the hash computation.

Editorial note: should or shall? Or "shall" for annex QES only?

8.6 Signature augmentation report

SVR-8.6-01 The signature augmentation report shall indicate one of the three results defined in ETSI TS 119 101 [1] clause 8.3.1

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

(*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 Organisation 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 is whished);*
- *the terms and conditions;*

one of the above document must identify the supported signature validation policies, if they are not provided in signature applicability rules (with formal OID/URI identification)

- *risk assessment and Information security policy*

In addition, the TSP can publish signature applicability rules.

NOTE: The description of any business (application) domain or any transactional context is to be found in such "signature applicability rules" document (not to be necessarily present in SVS Practice Statement)

2. Trust Service management and operation

Editorial note: this clause may be common to any services offered by the TSP – except for CA that should follow the RFC 3647's ToC.

(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

(shall identify a.o. the obligations of all external organizations supporting the TSP services including the applicable policies and practices (per ETSI EN 319 401)
2.2.2 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

3.1 Signature validation process requirements

This clause shall contain requirements, control objectives and controls in connection with clause 8.1. in 119 441.

3.2 Signature augmentation process requirements

This clause shall contain requirements, control objectives and controls in connection with clause 8.2. in 119 441.

3.3 Signature validation / augmentation protocol requirements

This clause shall contain requirements, control objectives and controls in connection with clause 8.3. in 119 441.

3.4 Interfaces

This clause shall contain requirements, control objectives and controls in connection with clause 8.4. in 119 441.

3.4.1 SVSP – client

3.4.2 SVSP – other TSP

3.5 Validation report requirements

This clause shall contain requirements, control objectives and controls in connection with clause 8.5. in 119 441.

Annex B (normative): Validation and augmentation of QES as specified in the EU Regulation

(Editorial note: this annex is to be completed and reviewed to check if all technical requirements needed on top of the main document are provided / then check that the informative table that maps requirements from this annex and from the main document to the Regulation Requirements is complete)

(question is it necessary to also specify AdES_QC in addition to QES?)

VPR-B-01 the signature validation process shall check that the certificate that supports the signature bears attribute(s) that claim that the certificate has been issued as a qualified certificate and shall confirm such assertions(s) by inspecting the issuing TSP qualifications in the trusted list of the member state where the issuing TSP operates.

VPR-B-01_bis the signature validation process shall be able to determine if the certificate that supports the signature is a qualified certificate for electronic signature or a qualified certificate for electronic seal.

VPR-B-02: the signature validation process shall check if the certificate that supports the signature bears an indication that the signatory's name is a pseudonym.

SVR-B-03: the validation shall report that the signatory's name is a pseudonym when it is the case.

VPR -B-04: the signature validation process shall check that the certificate that supports the signature bears attribute(s) that claim the certificate is stored in a qualified electronic signature creation device, and if there is no assertion on this claim, shall search for such assertions(s) by inspecting the issuing TSP qualifications in the trusted list of the member state where the issuing TSP operates.

VPR-B-05: in order to satisfy VPR-B-01 to VPR-B-04 the implementation should comply with ETSI TS 119 172-4 [i.12]

NOTE 1 : ETSI TS 119 172-4 [i.12] also support a signature validation process that allows the implementation verify that an AdES is an AdES_QC.

NOTE 2 : ETSI TS 172-4 [i.12] allows the implementation to proactively reports that an AdES is an AdES_QC or a QES

OVR-B-06: The signature validation policy shall clearly be identified as a validation policy for validating that a signature is an AdES_QC or a QES.

VPR-B-07: the timestamps used in augmentation process shall conform to ETSI EN 319 422 [i.14] .

NOTE: There is no obligation to have qualified timestamps for QES – this is an added value for SVSP that offers augmentation for QES.

SVR-B-08: The validation report shall clearly indicate when the SVS did not performed the hash computation.

NOTE: when the client computes the hash this cannot be ensured by the SVSP and left to the responsibility of the client.

SVR-B-09 the validation report shall indicate whether the QES is a qualified electronic signature or a qualified electronic seal.

Annex C (normative): Qualified Validation Service as defined by the EU Regulation

Editorial note: to complete and review

VPR-C-01 The QTSP offering qualified validation of QES shall abide to requirements of Annex B

SVR-C-02 The validation report shall bear the advanced electronic signature or advanced electronic seal of the SVSP.

Editorial note; when the report is presented through a web interface, do we allow to have a SSL authentication supported by a QWAC and have no actual seal or signature on the report itself? Authenticating a data with a QWAC can be considered as "sealing" the data, however, the validation response (even if so "sealed") is not exactly the validation report.

SVR-C-03 [CONDITIONAL] when the validation report is presented through a webpage the SVSP should be authenticated within a TLS session supported by a QWAC certificate.

SVR-8.5-04 The validation report shall be provided to the client in an automated manner.

Editorial note: is it possible for a SVS that it is not provided in an automated way?

SVR-8.5-05 The validation report shall be provided to the client in a reliable manner.

SVR-8.5-6 The validation report shall report on the quality of the timestamps (i.e. qualified or not).

SVR-8.5-07 The signature validation report shall bear the Validator Information under the form of a certificate that bear the name of the QTSP such as indicated in the official status.

SVR-8.5-08 The QSVSP shall be able to indicate whether a signature is fully conformant to the requirements of a Qualified Electronic Signature /Seal (as defined in Regulation), or an advanced electronic signature/seal based on a qualified certificate (AdES_QC).

SVR-8.5-09 The QSVSP may claim conformance to the present document and its Annexes B and C by using the specific service policy OID defined in clause 4.2.2.

Annex D (informative): Regulation and validation policy requirements mapping

The following table provides indication on how to satisfy the validation of QES as specified by the EU Regulation.

For the validation of qualified electronic seal the EU Regulation Article 40 is applicable. Article 40 states "*Validation .. of qualified electronic seals : Articles 32, .. shall apply mutatis mutandis to the validation .. of qualified electronic seals*"; the table below applies thus *mutatis mutandis* to the validation of qualified electronic seal, and the validation requirements relating to pseudonym are not applicable to electronic seals.

EU Regulation Article 32 - Requirements for the validation of qualified electronic signatures 1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:	**Applicable requirements**
(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;	VPR-B-01, VPR-B-01_bis, VPR-B-05 (+ the requirements listed below for Annex I compliance)
(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;	VPR-B-01, VPR-B-05 VPR-8.1-01
(c) the signature validation data corresponds to the data provided to the relying party;	VPR-8.1-01
(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;	SVR-8.5-07, SVR-B-03
(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;	SVR-B-03
(f) the electronic signature was created by a qualified electronic signature creation device;	VPR -B-04, VPR-B-05
(g) the integrity of the signed data has not been compromised;	VPR-8.1-01 (note: to have this verified along time, the correct signature class/levels is needed)
(h) the requirements provided for in Article 26 were met at the time of signing.	VPR-8.1-01 (the validation algorithm does not guarantee all elements of Article 26 – only (a) and (d) are

	covered and (d) requires the correct signature class/levels to be verified along time) VPR-B-01 (the fact that a TSP is qualified for issuing Q_Certs implies that it has been supervised to correctly cover Article 26 (b) VPR-B-04 (the fact that a device is qualified implies that it has been certified to correctly cover Article 26 (b))
2. The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and	VPR-8.1-01
shall allow the relying party to detect any security relevant issues.	VPR-8.1-02, SVR-8.5-01 (*editorial note: conformance to 119 102-2 is only a should in the main document – may be to be set as a shall in annex B)?*
Annex I; Qualified certificates for electronic signatures shall contain:	
(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;	VPR-B-01, VPR-B-01_bis
(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified certificates including at least, the Member State in which that provider is established and: — for a legal person: the name and, where applicable, registration number as stated in the official records, — for a natural person: the person's name;	Partly covered by SVR-8.5-02 and partly by VPR-B-01
(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;	SVR-8.5-07 SVR-B-03

(d) electronic signature validation data that corresponds to the electronic signature creation data;	VPR-8.1-01
(e) details of the beginning and end of the certificate's period of validity;	VPR-8.1-01
(f) the certificate identity code, which must be unique for the qualified trust service provider;	
(g) the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;	VPR-8.1-01
(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;	VPR-8.1-01
(i) the location of the services that can be used to enquire about the validity status of the qualified certificate;	VPR-8.1-01
(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.	VPR -B-04

Annex E (informative): Recommendations on user interface

Editorial note: to complete and review

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

E-01 The SVS should ensure that he user interface provides the result of the verification in a clear way to the user

E-02: 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: The user interface should be able to display the validation report

E-04: The user interface should be able to present the purported signer's identity, including:

a) the signer's certificate subject's distinguished name;
b) the distinguished name of the issuing CA; and
c) the distinguished name of the hierarchically superior CAs

E-05: The user interface should be able to present:

a) the signature validation policy used in the validation / augmentation process
b) any known commitment implied by the signature

(+ other signed attributes ?)

(+ should be able to refer to any Signature Applicability Rules document if applicable, e.g. with a clickable link)

E-06 the requirements specified in ETSI TS 119 101 [1], clause 5.1 should apply.

E-07 The validation report should be displayed to the client in an 'efficient' / 'user friendly' / 'understandable' manner.

Editorial note: to complete:

- *if the TSP delivers the report in the form of a PDF document, we can specify things about report representation*
- *the TSP could help the user to use the service in a secure manner, e.g. specify if some actions can be taken from client side*
- *a validation service can allow a client to input the "is the AdES a QES, or an AdES_QC" (e.g. as part of the constraints) or can pro-actively report on this quality.*

Annex F (informative): Checklist

Editorial note: a checklist similar to the EN 319 411-1/-2 could be provided

History

Document history		
V0.0.2	June 2017	Early draft
V0.0.3	November 2017	Stable Draft for ESI review before public availability (same content as ESI(17)000164)
V0.0.4	November 2017	Stable draft for public review