SERVICE POLICY AND PRACTICE STATEMENT

Policies and practices for signatures and seals validation service

SVS and QSVS

DOCUMENT CODE	ICERT-INDI-QSVS
VERSION	1.3
DATE	07/05/2025

tinexta infocert

CONTENTS

INDEX OF FIGURES

1 INTRODUCTION

1.1 Overview

An electronic signature is data attached to an electronic document or other data which provides an indication of a person's intent to agree to the content of the document or data to which the signature relates. An electronic seal is data attached to an electronic document or other data, which ensures data origin and integrity. An electronic time stamp is data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

This document is intended to describe the policies and operating procedures adopted by InfoCert S.p.A. (hereinafter, also simply "**InfoCert**") for the provision of the qualified trust service for validating qualified electronic signatures, seals, and timestamps (QSVS hereinafter) according to the eIDAS Regulation, as well as for the provision of the non-qualified trust service for validating electronic signatures, seals, and timestamps (hereinafter "SVS"). The structure of this document follows the recommendation of Annex A of ETSI TS 119 441.

The InfoCert validation service has been designed and developed in accordance with the standards listed in clause 1.5.

1.1.1 TSP identification

InfoCert S.p.A. is the provider of the SVS and QSVS. InfoCert is registered in the register of companies in Rome with national and VAT number 07945211006.

1.1.2 Supported signature validation service policy(ies)

The validation of qualified electronic signatures / seals / timestamps is always performed by the SVS and QSVS according to a signature validation service policy.

This document is associated with the validation service policies for signatures—qualified for QSVS and non-qualified for SVS—identified by the Object Identifiers (OIDs) described below.

The Object Identifier (OID) which identifies InfoCert is **1.3.76.36**

Name	Description
QSVSP – InfoCert Signature Validation Service Policy compliant with the qualified validation criteria of ETSI TS 119 441, including the requirements specified in Annex B.	1.3.76.36.1.1.90 according to 0.4.0.19411.1.2
SVSP – InfoCert Signature Validation Service Policy compliant with the validation criteria of ETSI TS 119 441, excluding the requirements specified in Annex B.	1.3.76.36.1.1.91 According to 0.4.0.19411.1.1

Table 1 – OID

Both the SVS and the QSVS use the following signature validation policy:

Name	Description	Compliance
Ad/Q-ESig Ad/QESeal Ad-ESigQC AdESealQc TL	Validates electronic signatures and seals, indicating whether they are Advanced electronic Signatures (AdESig), AdES supported by a Qualified Certificate (AdESigQC), Qualified electronic Signature (QESig) validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps), Advanced electronic Seals (AdESeal), AdES supported by a Qualified Seal (AdESealQC), Qualified electronic Seal (QESeal).	Compliant to the OID 0.4.0.191724.1.1 defined in ETSI TS 119 172-4 [7]

Table 2 – Signature validation policy:

The existence of the signature in a given instant of time (i.e. the PoE, Proof of Existence) is verified by considering the attached timestamp when present, otherwise by considering the signed attribute "signing time" of the signature. In case the latter is also absent, the validation instant of the signature by the SVS or QSVS shall be considered as the time instant.

1.2 Signature Validation Service Components

1.2.1 SVS actors

The activities, both of SVS and QSVS, include the participation of the following actors:

- the signer, in consideration that the signature validity can be limited/influenced by the usage of signature creation policies or invalid signing certificates;
- the QTSP that has issued the signing certificates;
- the QTSP that has issued the timestamping certificates;
- the European member states trusted list providers;
- the European Commission that provides the list of trusted lists.

1.2.2 Service architecture

Two functionalities are provided for SVS and QSVS:

- The validation of a signed and/or timestamped document;
- The validation of a certificate, i.e. the verification that a given certificate is not expired, suspended or revoked at the time of the validation request.

Regarding the document validation, **SVS and QSVS perform** the check of the signature format, the identification of the signing certificate(s), the validation context initialization, the check of the revocation freshness, the X.509 certificate validation, the cryptographic validation and the signature acceptance validation according to ETSI EN 319 102-1 requirements.

SVS and QSVS implement the signature validation protocol on the server side. In particular:

- executes the signature validation service protocol and processes the signature validation on the SVSP side;
- runs the signature validation application (SVA) that implements the validation algorithm defined in ETSI EN 319 102-1. For this purpose, the service can call external actors e.g.:
  - The CA having issued the signing certificate (for certificate(s) status information or to get a CRL)
  - The CA of the TSA(s) that have provided timestamps within the signature.
  - The EU Member States trusted lists, the List of Trusted Lists of the European Commission (in the case of QSVS)
  - and/or other trusted lists (in the case of SVS)
- creates the signature validation report(s) related to the request;
- builds the signature validation response.

Regarding the certificate validation, **SVS and QSVS perform** the X.509 certificate validation using the validation algorithm defined in ETSI EN 319 102-1. The service can call external actors, for example the CA that issued the signing certificate, to obtain certificate status information or to verify the certificate chain, or the OCSP and CRL remote services to verify the certificate status.

1.2.3 Process

SVS and QSVS receive signature and/or certificate validation requests and return their responses to the requesting clients. The response can be provided synchronously or asynchronously. The communication channel between the clients requesting signature validation and the SVS or QSVS ensures the authentication of the SVS/QSVS and may also support client authentication.

SVS and QSVS invoke other TSP services only to retrieve the status of signing and/or timestamping certificates.

The process performed by QSVS/SVS can be divided in the following steps.

Step 1. SVS and QSVS receives a signature validation request.

In case of a signature validation request, 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.
3. (optional) Validation constraints, as defined in ETSI EN 319 102-1.

In case of a certificate validation request, the request includes:

4. The Base64-encoded certificate;
5. (optional) Validation constraints, as defined in ETSI EN 319 102-1.

Step 2. SVS and QSVS perform the validation process.

The validation process is compliant to ETSI EN 319 102-1 specification.

Validation is carried out by the SVSP/QSVSP according to constraints that can be provided either by the client requesting the signature validation and/or by the service itself.

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

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

Step 3. SVS and QSVS prepares and sends the validation response.

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

The validation report is compliant to ETSI TS 119 102-2 specification. It is sealed by an InfoCert eSeal certificate. It 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.

There is one validation report for each validated digital signature.

1.3 Definitions and abbreviations

1.3.1 Definitions

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

(signature) validation constraint: technical criteria against which a digital signature can be validated

signature validation policy: set of **signature validation constraints** processed or to be processed by the Signature Validation Application (SVA)

1.3.2 Abbreviations

Descrizione	OID
0.4.0.19441.1.1	SVSP conforming ETSI TS 119 441 OID
0.4.0.19441.1.2	QSVSP conforming ETSI TS 119 441 OID
DA	driving application: in ETSI EN 319 102-1, application that

Descrizione	OID
	uses a Signature Validation Application (SVA) in order to validate digital signatures
QSVS	Qualified Signature Validation Service
QSCD	Qualified Signature/Seal Creation Device
QSVSP	Qualified Signature Validation Service Provider
QSVSPS	Qualified Signature Validation Service Practice Statement
(SVS) policy and practice statement	set of rules or/and practice statement that indicates the applicability of a signature validation service to a particular community and/or class of application with common security requirements
SVSP	Trust Service Provider (TSP) that performs the validation of a digital signature is called a Signature Validation Service Provider
SVR	Signature Validation Report The outcome of SVS
SVA	signature validation application: in ETSI EN 319 102-1, 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
SVS	Signature Validation Service
SD	Signer's document
SDO	Signed Data Object
SDR	Signer's Document Representation

Table 3 – Abbreviations

1.4 Policies and practices

1.4.1 Organization administrating the TSP documentation

InfoCert is responsible for the administration of the set of practices of the InfoCert SVS and QSVS.

InfoCert is responsible for defining, updating and publishing this document.

InfoCert reserves the right to make changes to this document for technical reasons or for procedures' updates that have occurred both due to laws or regulations, and for optimizations of the work cycle. Each new version of the Operating Manual cancels and replaces the previous versions. Variations that do not have a significant impact on users lead to an increase in the release number of the document, while variations with a significant impact on users (such as significant changes to operating procedures) lead to an increase in the version number of the document. In any case, the manual will be promptly published and made available to users.

The procedures for reviewing the Operating Manual are like the drafting procedures. The revisions are made in agreement with the Certification Service Manager, the Security Manager, the Privacy Manager, the Legal Department, the Consulting Area and are approved by the management.

These SVSPS and QSVSPS will be reviewed at least once a year, and they are published in English on InfoCert's corporate website.

Information	Description
Version/Release:	**1.3**
Version/Release date	**07/05/2025**
Description of changes:	**Update of Logo and Operational and Legal Office – Rome** **CPS Revision Integrating SVS and QSVS** **InfoCert Phone Contact Update** **General Review of Document Styles and Formats**
Reasons:	**General document review, accessibility, updates, corrections, and introduction of non-qualified validation (SVS)**

Table 4 – Version 1.3

Informazione	Dettaglio
Version/Release n°:	**1.2**
Version/Release date:	**04/06/2024**
Changes' description:	§ 1.4.1 moved content from 1.4.3; § 1.4.3 added content according to Annex A; § 2.1.1 added AWS sub-contractor; § 2.6 updated versions of cryptographic libraries; **Added the Appendix A with documentation about testing.**
Reasons:	**revision of the document for reorganization of contents according to Annex A**

Table 5 – Version 1.2

Informazione	Dettaglio
Version/Release n°:	**1.1**
Version/Release date:	**14/04/2024**
Changes' description:	2 description of the signature validation policy and of the Proof of Existence; § 1.2 added the validation of a certificate; **Company logo update**
Reasons:	**revisione del documento per riorganizzazione contenuti secondo Annex A**

Table 6 – Version 1.1

Informazione	Dettaglio
Version/Release n°:	**1.0**
Version/Release date:	**22/02/2024**
Changes' description:	first issue
Reasons:	first issue of the document

Table 7 – Version 1.0

1.4.2 Contact person

For questions, complaints, comments, and requests for clarification regarding this Service Practice Statement, please contact:

Company name	**InfoCert – S.p.A.** **Responsabile del Servizio di Certificazione Digitale**
Phone	*0683669635*
Contact Center	**https://help.infocert.it/contatti/**
Website	**https://www.firma.infocert.it**, **https://www.infocert.it**
E-mail	**firma.digitale@legalmail.it**

1.4.3 TSP (public) documentation applicability

See document heading and paragraph 1.1.2.

The documentation relating to the validation services is composed of the following objects:

- the current CPS, or Operating Manual, ICERT-INDI-QSVS, identified by OID 1.3.76.36.1.1.90 for QSVS and 1.3.76.36.1.1.91 for SVS. The latest version published on InfoCert's corporate website applies;
- the CGC, General Contract Conditions, which regulate the relationships with customers who subscribe to the service. The latest version published in the InfoCert corporate website applies;
- the service practices described in this CPS and defined in paragraph 1.1.2. The same paragraph also identifies the signature validation policies supported by SVS and QSVS, which are defined by a formal OID and also returned in the service responses;
- the risk analysis and the information security policies adopted (Security Checklist and Privacy Checklist), which are updated annually in the InfoCert document space, but not made public externally;
- the test plan and test reports with the results, as described in Appendix A.

1.5 References

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 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

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

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

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

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

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

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

[10] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[11] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile".

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

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

[14] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

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

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

[17] ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

[18] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[19] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[20] ETSI TS 119 182-1: "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

2 TRUST SERVICE MANAGEMENT AND OPERATION

2.1 Internal organization

The internal organizational structure supporting the activity of QTSP is described in document “Certified Electronic Mail Services and Digital Certification – Structure Organizational "(ICERT-CAPEC-ORG). The service is provided with an IT structure of InfoCert property and under the complete control and responsibility of InfoCert.

2.1.1 Organization reliability

As defined in the document “Trust Service Provider InfoCert – Certificate Practice Statement”, having ID ICERT-INDI-MO.

The signed data are never stored by the QSVS. The SVS and QSVS service is provided on AWS Cloud, which is a subcontractor managed according to the company policy.

2.1.2 Segregation of duties

The activities and tasks of QTSP personnel are defined and documented. The security organization system is based on a robust principle of security of the logical type (operators at various levels, system administrators, etc.).

The logical segregation of duties is provided by the control access system. For system administrators, logon and logoff operations are registered, as required by the GDPR. The retention time of such registrations is 6 months, registrations can be verified by non-admin people.

2.2 Human Resources

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

2.3 Asset Management

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

2.4 Access Control

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

2.5 Cryptographic Controls

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

In order to provide its service, the QSVSP needs to generate a key pair used to sign the validation reports.

Such keys are generated solely by staff specifically in charge of this function. Key and signature generation takes place within dedicated and certified cryptographic modules, as required by current legislation.

The certificate signing the validation report is issued by an InfoCert CA/QC service.

Protection of the QSVS private key is ensured by the key generation and cryptographic module usage. The private key can only be generated if two key generation employees are simultaneously present. Key generation takes place in the presence of the service manager.

QSVS private keys are duplicated for the sole purpose of being recovered after secure signature device breakdown. Duplication takes place through a controlled procedure by which the key and its context are duplicated on multiple devices as required by HSM device safety criteria.

The cryptographic module used for key generation and signature complies with requirements that ensure:

- compliance of the key pair with minimum requirements imposed by the generation and verification algorithms used;
- a fair probability of generation of possible key pairs;
- identification of the subject activating the generation procedure;
- that signature generation takes place inside the device so that the value of the private key being used cannot be intercepted.

2.6 Physical and environmental security

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

The cryptographic libraries used by the SVS and QSVS allow to manage the cryptographic algorithms and sizes defined in ETSI TS 119 312. Dss-framework 6.0 and bouncycastle 1.77 cryptographic libraries are being used.

2.7 Operation security

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

The operating system of computers used in validation activities involved in key generation, signatures validation and creation are hardened, i.e. they are configured to minimize the impact of any vulnerabilities by eliminating features that are not required for SVS and QSVS operations and management.

System administrators appointed for this purpose in accordance with applicable regulations shall access the system by means of a root on demand application, that enables root user privileges to be used only after individual authentication. Each access is traced, logged and stored for 12 months.

The libraries used in validation operations are well tested and regularly reviewed and updated, above all checking eventual announcements of bugs or vulnerabilities.

SVS and QSVS use secure protocols such as Transport Layer Security or connection through a secure VPN so that any sensitive data is protected by encryption, moreover a policy regarding key strength and key management is defined and implemented according to ETSI TS 119 312 requirements.

2.8 Network security

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

The QSVS does not store any confidential data and does not perform any connection to systems storing or processing confidential data.

2.9 Incident management

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

2.10 Collection of evidence

Records for each major SVS ad QSVS event are drawn up and archived. Event logs are collected and archived in the InfoCert preservation system according to the methods described in the preservation system security manual. Event logs are stored for a 7 years period in the InfoCert preservation system.

2.11 Business continuity management

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

In the case of QSVS, signature validation reports are digitally signed and include signatures timestamps. Any further augmentations of the validation reports signatures, in order to be validated over the long term are responsibility of the subscribers.

2.12 TSP Termination and Termination Plans

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

2.13 Compliance

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.

No personal data are processed by a third party. After processing completion signed data are never stored by the SVS and QSVS.

3 SIGNATURE VALIDATION SERVICE DESIGN

3.1 Signature validation process requirements

InfoCert SVS and QSVS allow a subscriber to provide signed data and/or signatures to be validated via an API. The QSVS performs the validation processing according to the validation algorithm defined in ETSI EN 319 102-1. The validation on AdES/QC and QES requirements is performed according to ETSI TS 119 172-4 signature validation policy. Via the same above-mentioned API, an XML-formatted validation report will be returned to the subscriber, which in the case of QSVS is also sealed with an InfoCert qualified electronic seal certificate whose private key is protected by a QSCD.

In the figure below, extracted from ETSI EN 319 102-1, there is a representation of the basic building blocks that are used to implement the validation algorithm and of the way these blocks are related to achieve signatures validation.

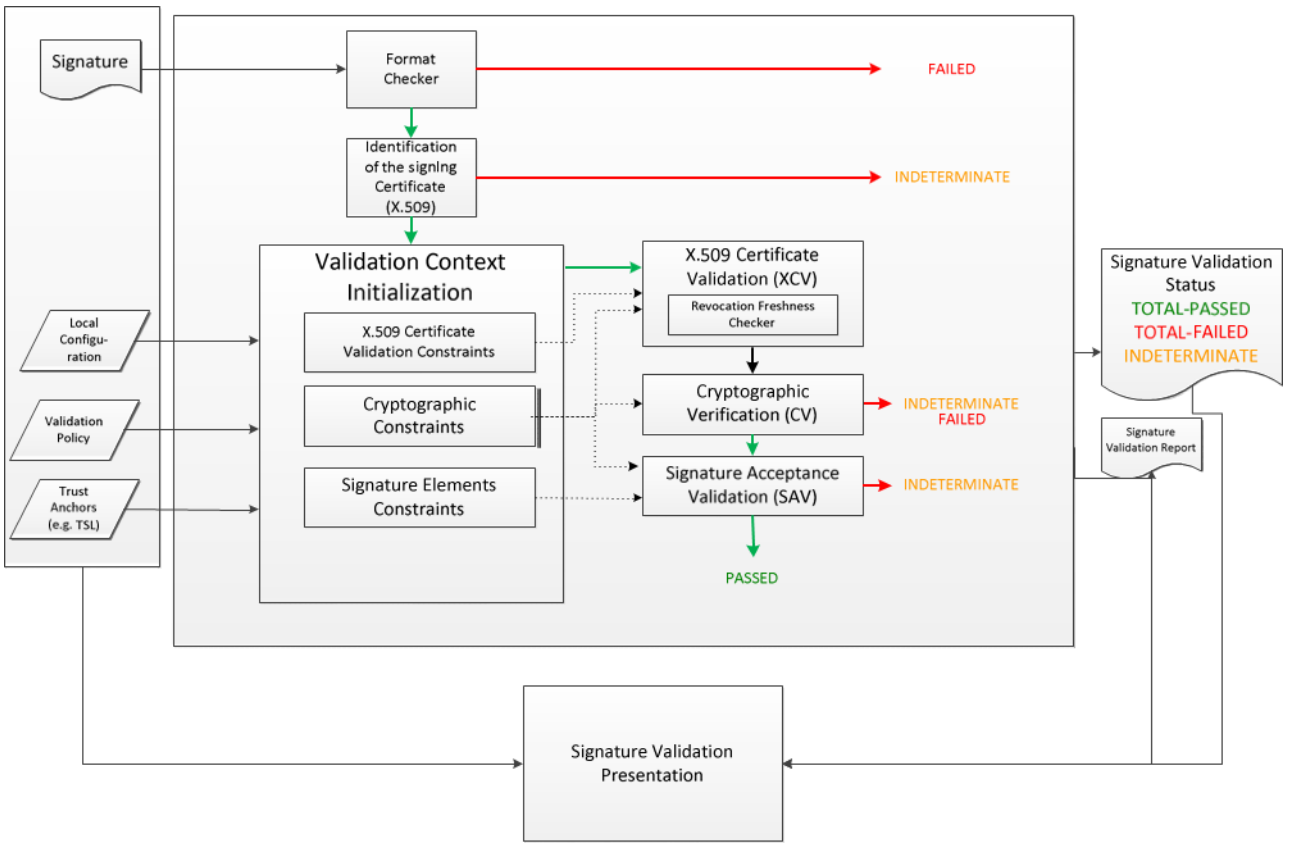


Figure 1 – Basic Signature Validation

InfoCert SVS andQSVS support only one signature validation policy that allows to validate AdES/QC and QES according to ETSI TS 119 172-4.

InfoCert SVS and QSVS support the validation of the following signature formats: ETSI TS 103 172 and ETSI EN 319 142 for PAdES, ETSI TS 103 171 and ETSI EN 319 132 for XAdES, ETSI TS 103

173 and ETSI EN 319 122 for CAdES, ETSI TS 103 174 and ETSI EN 319 162 for ASiC, ETSI TS 119 182-1 for JAdES.

The process performed by the SVS and QSVS can be divided in the following 4 steps.

1. The QSVS receives a signature validation request. The request shall include:
    a. the SDO with the embedded signature(s) or
    b. the SD and the corresponding detached signatures.
2. SVS and QSVS perform the validation process according to the ETSI EN 319 102-1 specification.
3. SVS and QSVS prepare the sealed validation report in accordance with the ETSI TS 119 102-2 specification and includes it in the signature validation response.
4. SVS and QSVS send the signature validation response to the subscriber requesting the signature validation.

A probe checks the integrity of the SVS and QSVS components on a daily basis. In case of detection of unauthorized modification of critical SVS and QSVS components, like for example configuration files, such components are repaired or disabled until their repair is possible.

3.2 Signature validation protocol requirements

It is not possible for the subscriber to provide a signature validation policy.

The subscriber shall:

- invoke the InfoCert SVS/QSVS via the provided API;
- in the case of QSVS, verify the qualified electronic seal on the validation report.

Parties relying on the QSVS service should:

- validate the qualified electronic seal on the validation report.

3.3 Interfaces

According to the conceptual model of the signatures / timestamps validation process defined in ETSI EN 319 102-1, the SVA receives requests from a DA as shown in the figure below extracted from ETSI EN 319 102-1.

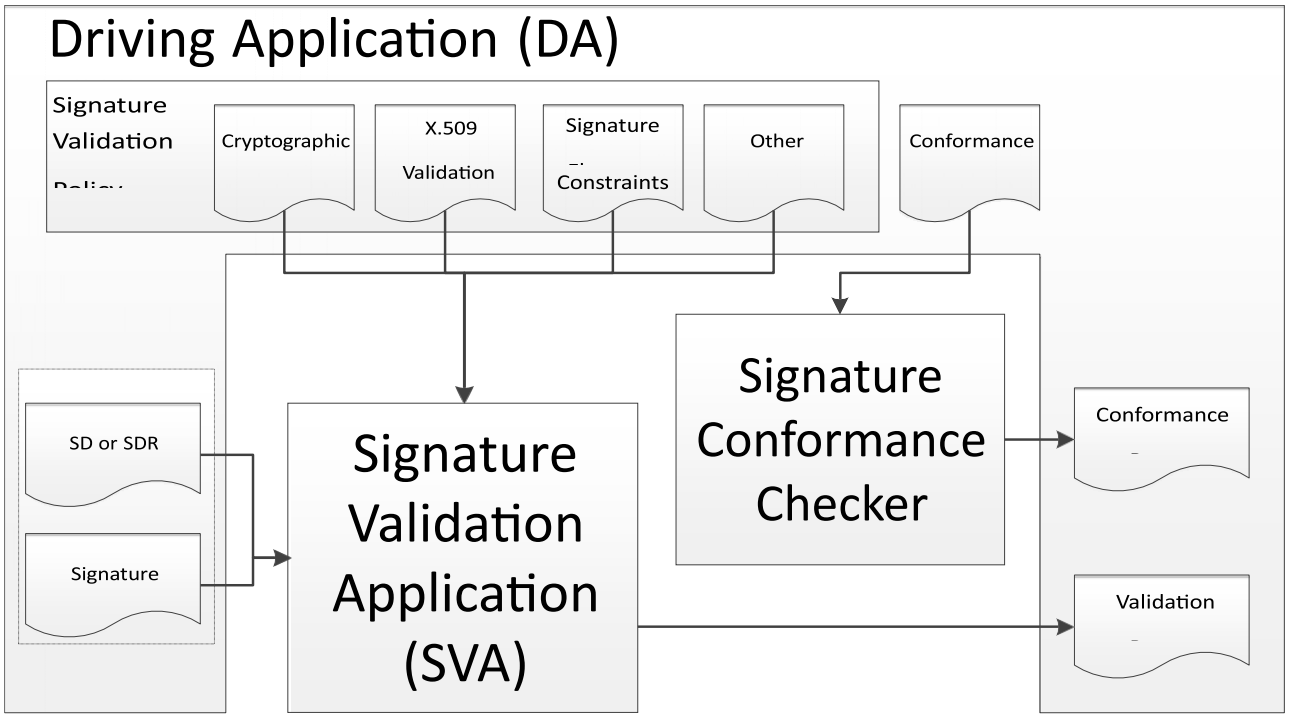


Figure 2 – Conceptual Model of Signature Validation

At the moment, the subscriber can pass the SD/SDR and/or the signature but is not allowed to provide any other input for the validation process (that's any element that can parameterize the validation process, such as constraints or conformance requirements).

SVS and QSVS use secure protocols such as Transport Layer Security or connection through a secure VPN. Therefore, the communication channel between the DA and the SVS and QSVS is secured allowing the SVS/QSVS to be authenticated by the DA and any data exchanged to be protected by encryption ensuring data confidentiality. SVS and QSVS do not store the SD/SDR or signature.

3.3.1 Communication channel

The communication channel between the DA (client) and the SVS/QSVS carries the signature validation request and the response. It is synchronous. It allows SVS/QSVS authentication via the TLS Communications Protocol. Deprecated versions of the protocol are not accepted. The subscribers of the SVS and QSVS are authenticated.

The SVS/QSVS queries OCSP status data and/or CRLs by means of the URLs embedded in the signing certificates authority information access and cRLDistributionPoints extensions.

3.3.2 SVSP - other TSP

In order to perform the service provision the SVS/QSVS, when checking for revocation, may need to communicate with other QTSPs querying their OCSP services and/or CRL distribution points. Primarily the OCSP protocol is used; if the interface is not available or does not provide relevant responses, a CRL distribution point, if available, is used.

The OCSP validation service is affected by the practices, policies and SLAs of other QTSPs that

are not under the control of InfoCert.

3.4 Signature validation report requirements

SVS and QSVS in their response to a signature validation request provide a status indication and a validation report being compliant to ETSI TS 119 102-2. According to the results of the signature validation processing, the signature validation report will indicate one of the three status (TOTAL-PASSED, TOTAL-FAILED, INDETERMINATE) and the relevant sub-indications as defined in ETSI EN 319 102-1. The signature validation report indicates the usage of an implicit signature validation policy for the validation of QES, AdES QC, qualified timestamps, timestamps recognized at national level and of the relevant validation constraints. The signature validation report includes:

- the identity of InfoCert S.p.A. as QSVSP reporting the following information:
  - X509Certificate
  - X509SubjectName
  - Ds:KeyValue
  - X509SKI
  - TSP Name
  - TSP Postal and Electronic Address
  - TSP Information URI
- the signer's identity
- an indication of any signed attributes
- an indication of the validation process performed
  - validation process for basic signatures
  - validation process for signatures with time and signatures with long-term validation material
  - validation process for signatures providing long term availability and integrity of validation material
- an indication of the quality of timestamps, if present in the signatures being validated
- an indication about the subject that performed the hash computation
- an indication that the origin of each POE is from withing the signatures

In the case of QSVS, the signature validation report is sealed by means of a qualified electronic seal certificate registered to InfoCert. Such electronic seal is a XAdES-B-T signature.

APPENDIX A

The test plan is described using the Gherkin language. Each type of signature validation is contained in a feature file. Each feature contains one or more test scenarios. An example of a feature file containing validation scenarios for CADES signatures is the following:

```
Feature: FUN.2.0: Validate CADES signed files

 Background:
   Given I authenticated on the identity provider
   And I received an authorization token

 Scenario Outline: FUN.2.0.<funCode>: validate <type>
   When I validate a signed file of type "<type>"
   And I get a validation result
   Then I generate the validation report
   And I check the result is successful

   Examples:
   | funCode | type                          |
   | 1       | cades-b-enveloping            |
   | 2       | cades-t-enveloping            |
   | 3       | cades-lta                     |
   | 4       | cades-t-detached-full-content |
   | 5       | cades-t-detached-digest       |
```

The test scenarios include the following types of signature validations:

- cades-b-enveloping
- cades-t-enveloping
- cades-lta
- cades-t-detached-full-content
- cades-t-detached-digest
- pades-b-invisible
- pades-t-invisible
- pades-lta-invisible
- pades-b-2-fields
- pades-t-2-fields
- pades-lta-2-fields
- xades-b-enveloping
- xades-t-enveloping
- xades-lta-enveloping
- xades-b-enveloped
- xades-t-enveloped

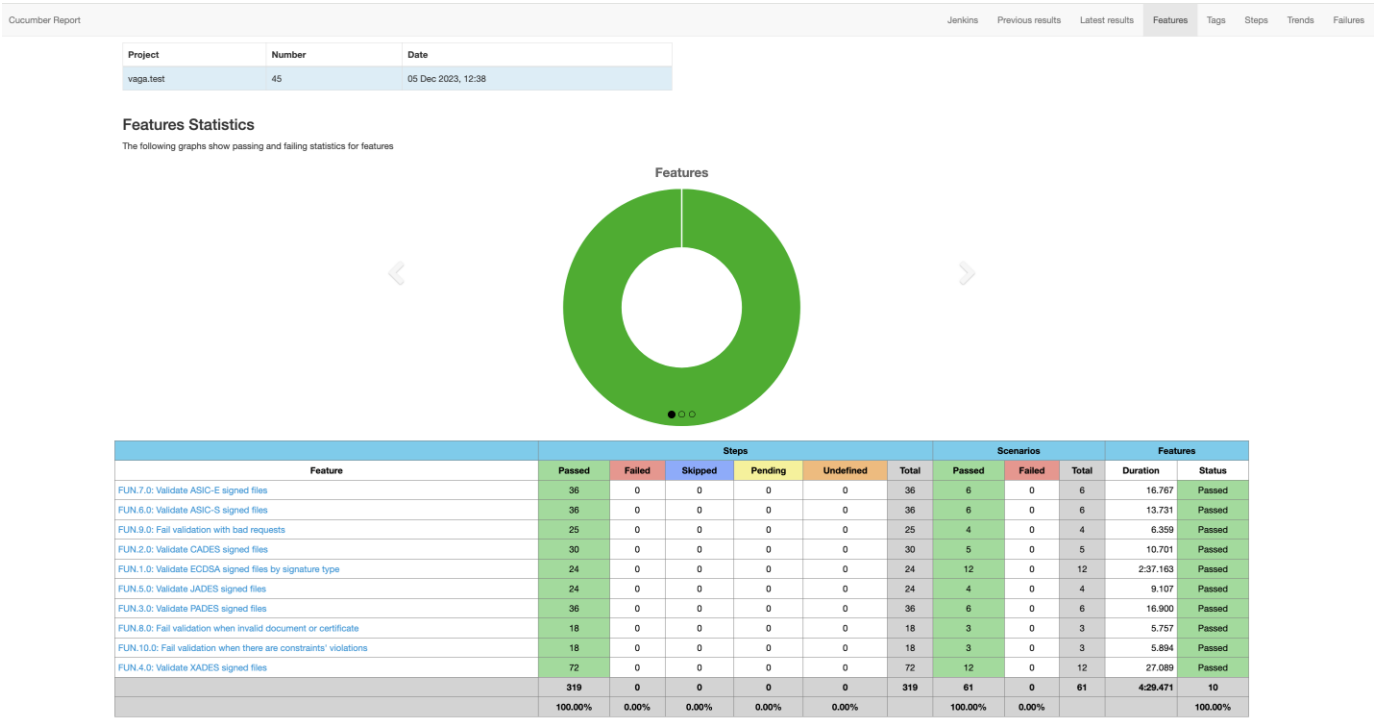
- xades-lta-enveloped
- xades-b-detached
- xades-t-detached
- xades-lta-detached
- xades-lta-detached-multiple-files
- xades-lta-enveloping-multiple-files
- xades-epes
- jades-t-enveloped
- jades-lta-enveloped
- jades-t-detached
- jades-lta-detached
- asic-s-xades-b
- asic-s-xades-t
- asic-s-xades-lta
- asic-s-cades-b
- asic-s-cades-t
- asic-s-cades-lta
- asic-e-cades-b
- asic-e-cades-t
- asic-e-cades-lta
- asic-e-xades-b
- asic-e-xades-t
- asic-e-xades-lta

And validations with negative test scenarios:

- invalid-certificate
- expired-certificate
- untrusted-certificate
- document modified-after-signature
- bad-original-content-type-detached
- bad-original-content-name-detached
- unsigned-content
- bad-original-content-detached
- XCV violation revoked
- CV violation data-integrity
- SVO violation timestamp

Each step described in the scenario is implemented with the Cucumber framework in Java. When the test execution is launched via Maven command, all the features, all the scenarios and all the steps are executed. At the end of the execution, the results can be viewed. The tests can be run on either the SVS service or the QSVS service, which differ in the validation URL that is invoked.

The test report is summarized in the following image:

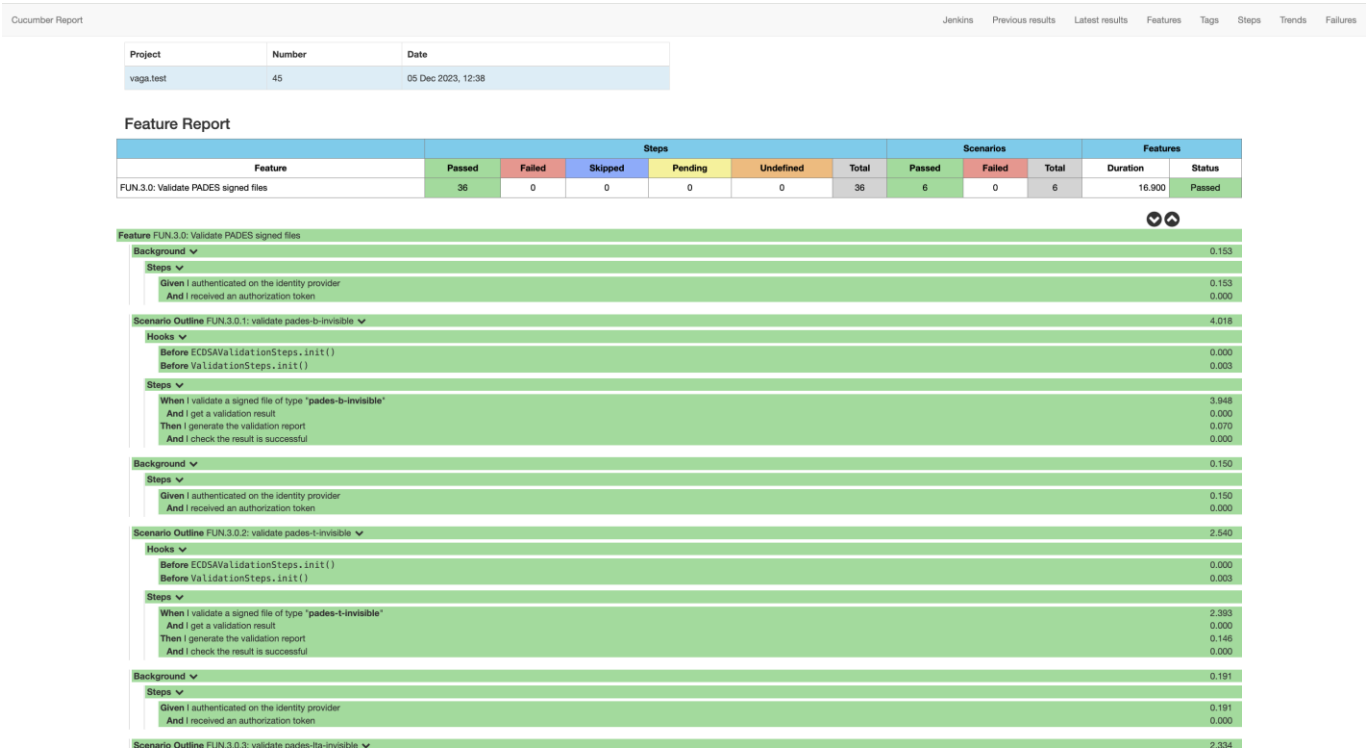


Feature	Steps						Scenarios			Features	
	Passed	Failed	Skipped	Pending	Undefined	Total	Passed	Failed	Total	Duration	Status
FUN.7.0: Validate ASIC-E signed files	36	0	0	0	0	36	6	0	6	16.767	Passed
FUN.6.0: Validate ASIC-S signed files	36	0	0	0	0	36	6	0	6	13.731	Passed
FUN.9.0: Fail validation with bad requests	25	0	0	0	0	25	4	0	4	6.359	Passed
FUN.2.0: Validate CADES signed files	30	0	0	0	0	30	5	0	5	10.701	Passed
FUN.1.0: Validate ECDSA signed files by signature type	24	0	0	0	0	24	12	0	12	2:37.163	Passed
FUN.5.0: Validate JADES signed files	24	0	0	0	0	24	4	0	4	9.107	Passed
FUN.3.0: Validate PADES signed files	36	0	0	0	0	36	6	0	6	16.900	Passed
FUN.8.0: Fail validation when invalid document or certificate	18	0	0	0	0	18	3	0	3	5.757	Passed
FUN.10.0: Fail validation when there are constraints' violations	18	0	0	0	0	18	3	0	3	5.894	Passed
FUN.4.0: Validate XADES signed files	72	0	0	0	0	72	12	0	12	27.089	Passed
	319	0	0	0	0	319	61	0	61	4:29.471	10
	100.00%	0.00%	0.00%	0.00%	0.00%		100.00%	0.00%			100.00%

Figure 3 – Test Report

Successfully executed features are highlighted in green, any failures are highlighted in red.

By clicking on each feature, it is also possible to see the execution details of each scenario and each step:



Feature	Steps						Scenarios			Features	
	Passed	Failed	Skipped	Pending	Undefined	Total	Passed	Failed	Total	Duration	Status
FUN.3.0: Validate PADES signed files	36	0	0	0	0	36	6	0	6	16.900	Passed

Figure 4 – Test Features

In addition to these visual reports, each scenario execution produces a PDF containing the JSON response given by the SVS/QSVS and the related ETSI XML report for a more detailed consultation of the results of the tests performed.

The tests are automated and can be launched via the Jenkins Continuous Integration tool on each environment: test, stage and production. Before each new release of the SVS and QSVS, the tests are executed in the stage environment and the production release is approved only if all the tests terminated successfully.

Negative test cases are useful to verify the behavior of SVS and QSVS in the presence of obsolete or revoked elements, or in the presence of algorithms considered no longer valid (for a guide on algorithms and their validity, refer to [6] [i.14]). In these cases, the overall response of SVS and QSVS has the status TOTAL_FAILED, while the status of the signatures is INDETERMINATE with the related details in the error messages.

The "expired-certificate" test case has two obsolete elements: the signing certificate is expired and the signing algorithm is RSA with 1024-bit key length, which is no longer considered valid. The QSVS JSON response has the following error messages:


```
"messages": [
{
"level": "ERROR",
"section": "ADES",
"key": "BBB_XCV_SUB_ANS",
"value": "The certificate validation is not conclusive!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "BBB_XCV_ICTIVRSC_ANS",
"value": "The current time is not in the validity range of the signer\u0027s certificate!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "ASCCM_AR_ANS_AKSNR",
"value": "The algorithm RSA with key size 1024 is no longer considered reliable for
signature creation!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "TSV_IBSTBCEC_ANS",
"value": "The best-signature-time is not before the expiration date of the signing
certificate!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "PSV_IPSVC_ANS",
```

"value": "The past signature validation is not conclusive!"
},
{
"level": "WARNING",
"section": "ADES",
"key": "BBB_XCV_AIA_PRES_ANS",
"value": "The authority info access is not present!"
},
{
"level": "WARNING",
"section": "QUALIFICATION",
"key": "QUAL_IS_ADES_IND",
"value": "The signature/seal is an INDETERMINATE AdES digital signature!"
}
]

The complete response can be found in the PDF report ValidationResult-EXPIRED-CERTIFICATE.pdf, generated by the automatic test execution and also containing the signed ETSI XML report.

The “XCV violation revoked” test case has one revoked element: the signing certificate. The JSON response from QSVS has the following error messages:

"messages": [
{
"level": "ERROR",
"section": "ADES",
"key": "BBB_XCV_SUB_ANS",
"value": "The certificate validation is not conclusive!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "BBB_XCV_ISCR_ANS",
"value": "The certificate is revoked!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "ADEST_IRTPTBST_ANS",
"value": "The revocation time is not after best-signature-time!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "PSV_IPSVC_ANS",
"value": "The past signature validation is not conclusive!"
},
{
"level": "WARNING",
"section": "ADES",
"key": "BBB_XCV_AIA_PRES_ANS",

"value": "The authority info access is not present!"
},
{
"level": "WARNING",
"section": "QUALIFICATION",
"key": "QUAL_IS_ADES_IND",
"value": "The signature/seal is an INDETERMINATE AdES digital signature!"
}
]

The complete response can be found in the PDF report ValidationResult-REVOKED.pdf, generated by the automatic test execution and also containing the signed ETSI XML report.