Service policy and practice statement

(Signature, Seal Validation Service QSVS)
Servizio di convalida firme e sigilli QSVS

CODICE DOCUMENTO	ICERT-INDI-QSVS
VERSIONE	1.0
DATA	10/02/2022

InfoCert
TINEXTA GROUP

SOMMARIO

1 INTRODUCTION 3
1.1 Overview 3
1.1.1 TSP identification 3
1.1.2 Supported signature validation service policy(ies) 3
1.2 Signature Validation Service Components 3
1.2.1 SVS actors 3
1.2.2 Service architecture 4
1.2.3 Process 4
1.3 Definitions and abbreviations 5
1.3.1 Definitions 5
1.3.2 Abbreviations 5
1.4 Policies and practices 6
1.4.1 Organization administrating the TSP documentation 6
1.4.2 Contact person 6
1.4.3 TSP (public) documentation applicability 6
1.5 References 7
2 Trust Service management and operation 9
2.1 Internal organization 9
2.1.1 Organization reliability 9
2.1.2 Segregation of duties 9
2.2 Human resources 9
2.3 Asset management 9
2.4 Access control 9
2.5 Cryptographic controls 9
2.6 Physical and environmental security 10
2.7 Operation security 10
2.8 Network security 11
2.9 Incident management 11
2.10 Collection of evidence 11
2.11 Business continuity management 11
2.12 TSP termination and termination plans 11
2.13 Compliance 11
3 Signature validation service design 12
3.1 Signature validation process requirements 12
3.2 Signature validation protocol requirements 13
3.3 Interfaces 13
3.3.1 Communication channel 14
3.3.2 SVSP - other TSP 14
3.4 Signature validation report requirements 14

INDEX OF FIGURES

Figure 1 – Basic Signature Validation 12
Figure 2 - Conceptual Model of Signature Validation 13

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 for the provision of the qualified trust service for validating qualified electronic signatures, seals, and timestamps (QSVS hereinafter) according to eIDAS regulation. The document structure follows the recommendation of Annex A of ETSI TS 119 441.

The InfoCert validation service has been designed and developed according to the standards listed in the References clause.

1.1.1 TSP identification

InfoCert S.p.A. is the provider of the 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 QSVS according to a signature validation service policy.
This document is associated with the signature validation service policy identified by the Object Identifiers (OID) described below.
The Object Identifier (OID) which identifies InfoCert is **1.3.76.36**

InfoCert signature validation service policy compliant to ETSI TS 119 441 qualified validation criteria	1.3.76.36.1.1.90 according to 0.4.0.19411.1.2

1.2 Signature Validation Service Components

1.2.1 SVS actors

The operations of the QSVS includes the participation of:

- 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

The QSVS performs the check of the signature format, the identification of the signing certificate(s), the validation context initialization, the check of the tevocation freshness, the X.509 certificate validation, the cryptographic validation and the signature acceptance validation according to ETSI EN 319 102-1 requirements.
The QSVS implements the signature validation protocol on the server 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) 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 European Member States trusted lists, the List of Trusted Lists of the European Commission,
  - and/or other trusted lists.
- creates the signature validation report(s) related to the request;
- builds the signature validation response.

1.2.3 Process

The QSVS receives the signature validation requests and returns its responses to the requesting clients. The response can be provided synchronously or asynchronously. The communication channel between the clients requesting signatures validation and the QSVS covers the authentication of the QSVS and can support client authentication too.

The QSVS invokes other TSP services only for retrieving the status of the signing and/or timestamping certificates.

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

Step 1. The QSVS receives 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.

Step 2. The QSVS performs the validation process.

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

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

1. If not provided by the client request, the SVS implements a "default value" signature validation policy.
2. If provided by the client, then the client signature validation policy can be completed as requested by the SVSP practices.

Step 3. The 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

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 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

1.4 Policies and practices

1.4.1 Organization administrating the TSP documentation

The PKI team of InfoCert is responsible for the administration of the set of practices of the InfoCert QSVS.

1.4.2 Contact person

InfoCert is responsible for defining, updating and publishing this document. For questions, complaints, comments and requests for clarification regarding this Service Practice Statement, please contact:

InfoCert S.p.A.
Responsabile del Servizio di Certificazione Digitale
Piazza Luigi da Porto n.3
35131 Padova
Telephone number: +39 06 836691
Fax: + 39 049 0978914
Digital signature call center: + 39 06 54641489
Web: https://www.firma.infocert.it
e-mail: firma.digitale@legalmail.it

1.4.3 TSP (public) documentation applicability

See document heading and paragraph 1.1.2.
The body in charge of reviewing and approving this QSVSPS document is the InfoCert Governing Board. This QSVSPS will be reviewed at least once a year.
This QSVSPS is published in the corporate website of InfoCert in English language.

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.

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, registraions 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 QSVS allow to manage the cryptographic algorithms and sizes defined in ETSI TS 119 312. dss-framework 5.9 and bouncycastle 1.6.9 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 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.
The QSVS uses 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 or process 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

As defined in the Certificate policy & Certificate Practice Statement - ICERT-INDI-MO of the Trust Service Provider InfoCert.
Records for each major 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.
Validation reports are digitally signed and include signatures timestamps. Eventual 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 QSVS.

3 Signature validation service design

3.1 Signature validation process requirements

InfoCert QSVS allows a subscriber to provide signed data and/or signatures to be validated via an API (at the moment no human interface is available). 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, sealed with an InfoCert qualified electronic seal certificate whose private key is protected by a QSCD, will be returned to the subscriber.
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.

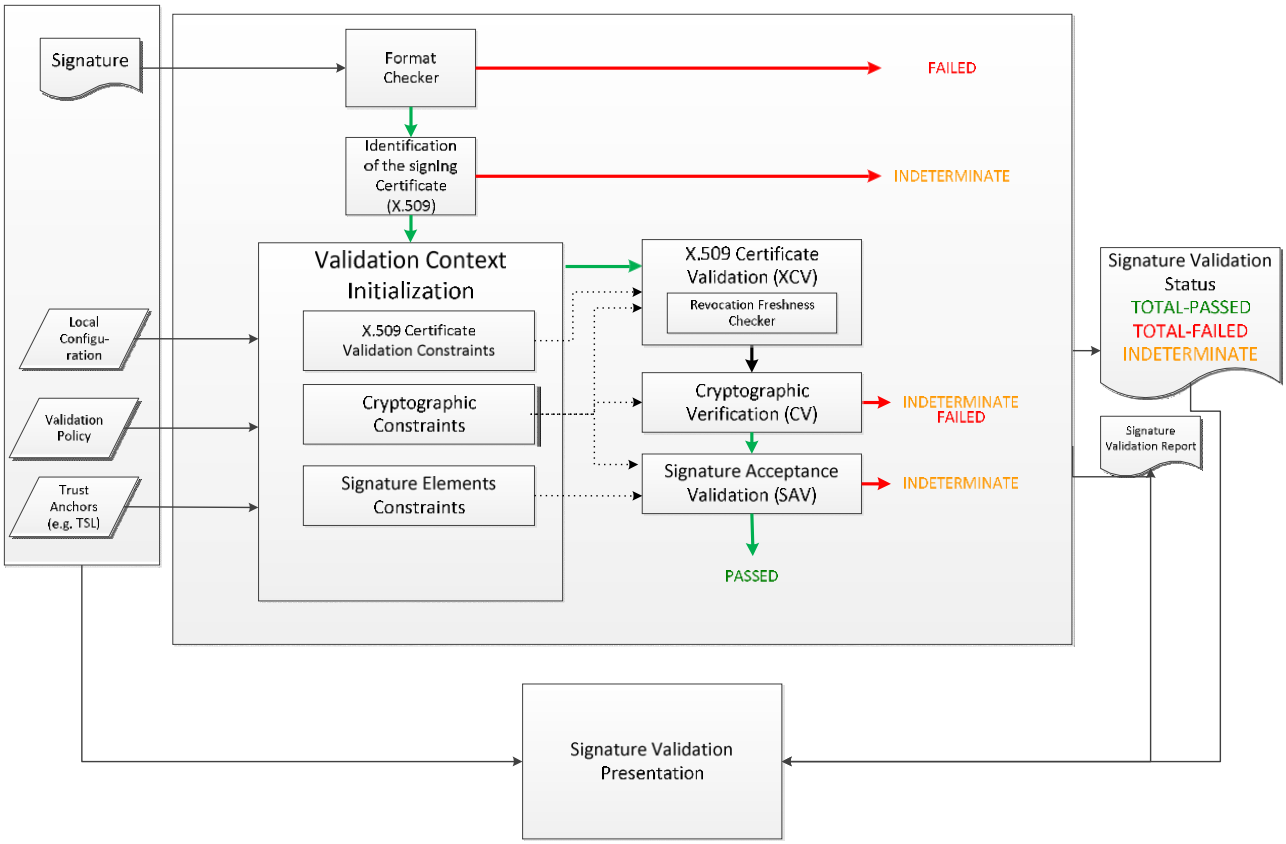

Figure 1 – Basic Signature Validation

InfoCert QSVS supports only one signature validation policy that allows to validate AdES/QC and QES according to ETSI TS 119 172-4.
InfoCert QSVS supports 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 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. The QSVS performs the validation process according to the ETSI EN 319 102-1 specification.
3. The QSVS prepares the sealed validation report in accordance with the ETSI TS 119 102-2 specification and includes it in the signature validation response.
4. The QSVS sends the signature validation response to the subscriber requesting the signature validation.

A probe checks the integrity of the QSVS components on a daily basis. In case of detection of unauthorized modification of critical 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 providing a signature validation policy.
The subscriber shall:

- invoke the InfoCert QSVS via the provided API;
- verify the qualified electronic seal on the validation report.

Relying parties 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.

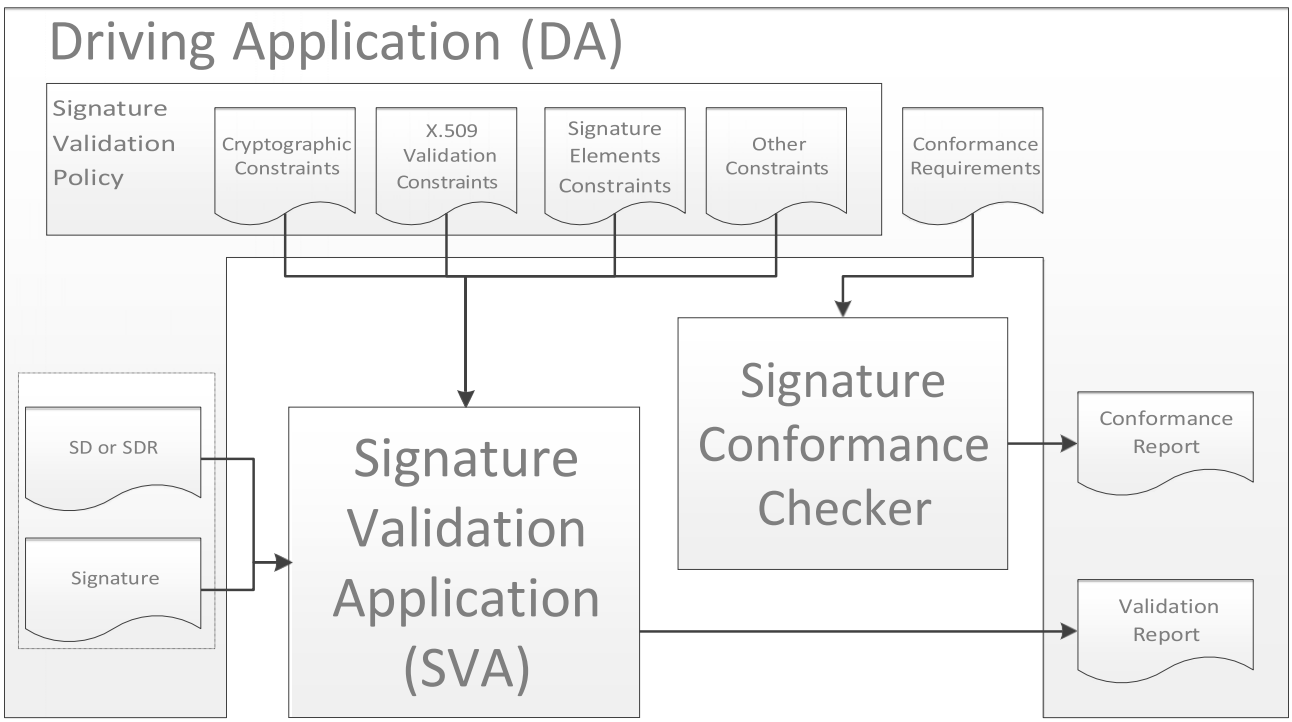

Figure 2 - Conceptual Model of Signature Validation

At the moment the subscribrer 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).
The QSVS uses secure protocols such as Transport Layer Security or connection through a secure VPN. Therefore the communication channel between the DA and the QSVS is secured allowing the QSVS to be authenticated by the DA and any data exchanged to be protected by encryption ensuring data confidentiality. The QSVS does not not store the SD/SDR or signature.

3.3.1 Communication channel

The communication channel between the DA (client) and the QSVS carries the signature validation request and the response. It is synchronous. It allows QSVS authentication via the TLS Communications Protocol. The subscribers of the QSVS are authenticated.
The 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 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 avaliable, 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.
When validating revocation of a certificate, compliance of the OCSP services with RFC6960 and of the other QTSPs with RFC5280 is assumed.

3.4 Signature validation report requirements

The QSVS in its response to a signature validation request provides 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

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.