APPROVED
PMO GOVERNANCE
DORU VIJIIANU
JUDIT FEKETE
MIRELA OJOG

Policy and Practice for Qualified Validation Service of Qualified Electronic Signatures/Seals (Policy and Practice for Signature Validation)

Edition history			
Edition	**Date and description of the change**	**Prepared**	**Approved**
1	20.10.2022 – First edition	Judit Fekete	Mirela Ojog
2	24.10.2023 -Second edition – Minor modification in chapter 2, 12.5.2, 9, 14.7, 14.9, 14.13	Judit Fekete	Mirela Ojog
3	24.04.2024 – Third edition	Judit Fekete	Mirela Ojog

ZIPPER

Contents

1. Introduction

This document is the Validation Policy of Zipper Services SRL [ZS], it establishes the validation rules for qualified and advanced electronic signatures (QES / AdES), and for qualified and advanced electronic seals (QEseal / AdESeal). It is in accordance with Regulation (EU) No. 910/2014 of the European Parliament and of the Council, and with section i.6 of the COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of September 8, 2015 (of in accordance with Article 27 and Article 37 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council):

> *"Advanced electronic signatures and advanced electronic seals are similar from the technical point of view. Therefore, the standards for formats of advanced electronic signatures should apply mutatis mutandis to formats for advanced electronic seals."*
>
> *AND*
>
> *"Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals".*

Policy for validating Electronic Signatures and Electronic Seals regardless of the legal type of the signature or seal (according to Regulation (EU) No 910/2014), i.e. the fact that the electronic signature or electronic seal is either Advanced electronic Signature (AdES), AdES supported by a Qualified Certificate (AdES/QC) or a Qualified electronic Signature (QES) does not change the total validation result of the signature.

The Public Key Infrastructure (PKI) of ZS CA is administered in accordance with the legal framework of Regulation [EU] 910/2014 of the European Parliament, and with Law 6/2020, of November 11, regulating certain aspects of the trusted electronic services from Romania.

This document has been prepared in accordance with current pan-European specifications and standards for the provision of trust services. Its structure follows the recommendation of **Annex A ETSI TS 119 441**.

2. Overview

The present document is entitled "Policy and Practice for Qualified Validation Service of Qualified Electronic Signatures/Seals" (Policy and Practice for Signature Validation Service). The purpose of the Policy and the Practice Statement is to meet the general requirements of the international community to provide trust and confidence in electronic transactions including, amongst others, the generally applicable requirements from Regulation (EU) No. 910/2014 establishing a legal framework for electronic signature and electronic seal, including their validation.

The present document specifies rules for establishing whether an electronic signature or electronic seal is valid based on the considerations specified in the present document and the validation constraints are applied to the verification procedures. In this perspective, the user and the relying party may address ZS, which, in its capacity as a qualified signature validation service provider (QSVP), will perform the validation of the digital signature on their behalf. The outcome of this procedure is a **signature validation report**. Participants of electronic transactions need to have confidence that ZS has properly established procedures and protective measures in order to minimize the operational and financial threats and risks associated with digital signatures.

The validation service validates all signatures and seals applied to the same input document and supplies resulting diagnostics in a single report, for all signatures/seals and applied timestamps. It does however not make any interpretation of supplied diagnostics or mutual relationship of those signatures and seals. In conclusion, the validation service does not allow the user to select the certificate(s) to be used for the validation. The client application, who will use the result of validation of those signatures and seals will interpret the result depending on the business context in which it is applied. Also, will allow to select, if necesarry, the specific signature to be verified in the case the verified content contains multiple signatures.

The validation policies specified in the present document are suitable for a large scope of application and business domains, whenever there is a need for validating electronic signatures or seals.

ZS provides the service in accordance with the requirements laid down in Regulation (EU) No. 91 0/2014 and guarantees that this service:

- Applies operational procedures and security management procedures that exclude any possibility for manipulation of the data and the status of the validated certificates; or
- Checks the validity of the electronic signature/seal in line with the requirements of Article 33 of Regulation (EU) No. 910/2014;
- Checks the status of the certificates in accordance with Recommendation RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- Validates qualified certificates and electronic signatures/seals: verifying qualification, integrity, authenticity and validity;
- Validates qualified electronic timestamps: verification of qualification, integrity, authenticity and validity;
- Fulfils the technical procedures for validation of signatures in line with the requirements of ETSI

There are three validation processes implemented, based on ETSI EN 319 102-1:

- The Validation process for Basic Signatures;
- The Validation process for Signatures with Time and Signatures with Long-Term Validation Material;
- The Validation process for Signatures providing Long Term Availability and Integrity of Validation Material, abbreviated in the report as "Validation Process for Signatures with Archival Data".

Those validation processes in turn rely on building blocks, which are denoted in ETSI EN 319 102-1 as:

- The basic building blocks;
- The time-stamp validation building block;
- The additional building blocks.

QSVP can provide additional information about the signature or the seal, e.g. if it is an advanced electronic signature/seal based on a qualified certificate.

In order to guarantee the proper functioning of the validation service, ZS tests each change in the validation service functionality and the tests are saved in the internal documentation of ZS. The tests are subject to verification and statements.

3. Policy Administration

Organization Administering this Document:
ZIPPER SERVICES
Strada Tăietura Turcului, Nr. 47, Imobilul Novis Plaza, Corp A, Et. 2,
Cluj-Napoca, 400285, România

Working Point:
B-dul 1 Decembrie 1918 nr. 1G,
Sector 3, Bucuresti, 032451, Romania

Working Point:
str. Nikola Tesla, nr. 2, cod 400221
Cluj-Napoca, 400285, Romania
https://ezipper.ro/en/

E-mail: office@ezipper.ro
Telephone +40 21.340.4638 / +40 31.101.1020
Fax: +40 21.340.4636 / +40 31.101.1022
(Mon-Fri 09.00. – 18:00 Eastern European Time)
Contact Person: Policy Administration Team

4. Policy Approval

Approval of this document and subsequent amendments are made by the persons dedicated by ZIPPER. These persons constitute the Policy Administration Team. PMC approves new versions of this document. Amended versions or updates shall be uploaded to the ZIPPER Repository located at https://pki.ca.ezipper.ro/repository/policies.php

Amended versions supersede any conflicting provisions of previous versions of this document. The Policy Administration Team (PMC) shall determine whether changes to this document require a change in the TS policy object identifiers of the Certificate policies.

5. NORMATIVE REFERENCES

ZS's Validation service has been designed and developed in accordance with:

- **ETSI EN 319 401**: General Policy Requirements for Trust Service Providers;
- **ETSI TS 119 441:** Policy requirements for TSP providing signature validation services;
- **ETSI TS 119 101:** Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for applications for signature creation and signature validation;
- **ETSI TS 119 442:** Protocol profiles for trust service providers providing AdES digital signature validation services;
- **ETSI TS 119 172-4**: (Draft) Signature policies, Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists;
- **ETSI EN 319 102-1:** Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation; 2;
- **ETSI TS 119 102-1:** Procedures for Creation and Validation of AdES Digital Signatures- Part 1: Creation and Validation;
- **ETSI TS 119 102-2:** Procedures for Creation and Validation of AdES Digital Signatures, Part 2: Signature Validation Report;
- **ETSI EN 319 122-1:** CAdES digitalsignatures, Part1: Building blocks and CAdES baseline signatures;

- **ETSI EN 319 122-2:** CAdES digitalsignatures, Part2: Extended CAdES signatures;
- **ETSI EN 319 132-1:** XAdES digitalsignatures, Part1: Building blocks and XAdES baseline signatures;
- **ETSI EN 319 132- 2:** XAdES digitalsignatures, Part2: Extended XAdES signatures;
- **ETSI EN 319 142-1:** PAdES digitalsignatures, Part1: Building blocks and PAdES baseline signatures;
- **ETSI EN 319 142-2:** PAdES digitalsignatures, Part2: Additional PAdES sign tures profiles;
- **ETSI EN 319 412:** (Electronic Signatures and Infrastructures (ESI): Certificate Profiles);
- **IETF RFC 3647:** "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- **ETSI TS 119 172-1:** Signature Policies, Part 1: Building blocks and table of contents for human readable signature policy documents;
- **ETSI TS 119 172-2:** Signature Policies, Part 2: XML format for signature policies;

6. TSP identification

Zipper Services SA [ZS] is the qualified service provider for the validation of qualified electronic signatures and seals (QSVSP) and is identified with a registered object identifier (OID):**1.3.6.1.4.1.57570.**

ZS ensures that it does not in any circumstances alter the object identifier of this document as well as the object identifiers of policies, practices and other referral documents. If there is an extension/update in policy and practice that will not affect previously issued certificates, ZS presents a new object identifier that covers the new certificates or extended/updated ones.

7. Supported signature validation service policy(ies)

The QSVSP works on the basis of a validation policy of signatures as input, that is, the validation of signatures / seals, is always performed against a validation policy. The validation policies accepted and whose requirements are used to carry out the process are:

ETSI TS 119 441 OIDs for Signature Validation Service Policy:

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

That is

- OID 0.4.0.9441.1.1 as the main policy OID for Signature Validation Services, and
- OID 0.4.0.9441.1.2 as the policy OID for Signature Validation Services that identifies qualified validation services as defined in articles Articles 32 and 33 of the Regulation UE 910/2014 (EIDAS)

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

Digital signature types

These OIDs indicate that the digital signature to which the OID is associated is a digital signature of the following corresponding type:

- EU qualified electronic signature - id-etsi-dst-euqesig - 0.4.0.191724.1.2.1

- EU qualified electronic seal - id-etsi-dst-euqeseal - 0.4.0.191724.1.2.4
- EU qualified electronic time stamp - id-etsi-dst-euqtst - 0.4.0.191724.1.2.7

8. Signature Validation Service Components

8.1. SVS actors

The two main actors are **ZS** (**QSVSP**) which is a qualified trust service provider (QTSP) and its **subscriber**.

The QSVP may offer one or more signature validation services based on contractual relations.

The electronic signature/seal validation service may be combined with other services for enhancing the signature reliability (e.g. timestamping, augmentation with qualified signature) in accordance with the protocol indicated in ETSI TS 119 442 which supports the order for enhancing the reliability of the signature with the validation service.

The subscriber is interacting with the application for signature validation and may be:

- an application or
- a human being (user)

Other actors in the provision of the signature validation services may be:

> The signer - the signer can set constraints on the signature (e.g. by means of a signature creation policy) and this may influence the signature validation;

> The signers' related trust service providers (TSP):

- The TSP having issued the signer's certificate (CA);
- Any TSP that can be implied in the signature generation:

> Other TSPs (TSAs; QSVSP, etc.)

> The European or foreign trusted list providers;

> The European Commission providing the trusted list of qualified service providers.

ETSI ESI has developed several standards to express signature applicability rules or "signature policy" in two **forms**:

- **In a human-readable form**: It can be assessed to meet the requirements of the legal and contractual context in which it is being applied (cf. ETSI TS 119 172-1).
- **In a machine processable form (XML or ASN.1):** To facilitate its automatic processing using the electronic rules (cf. ETSI TS 119 172-2 and ETSI TS 119 172-3).

9. Service architecture

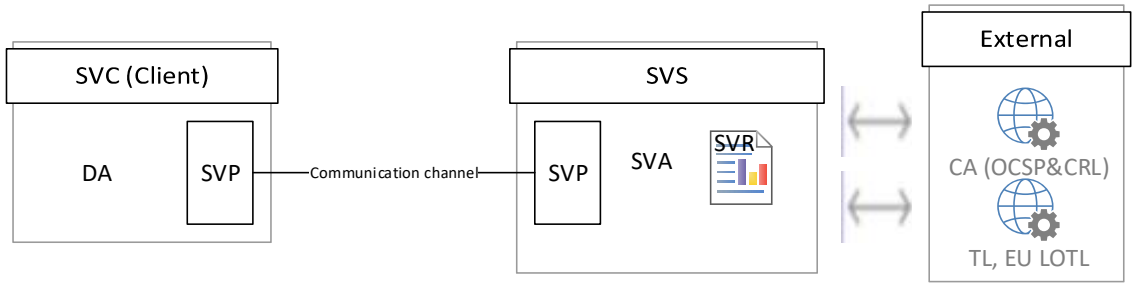
The signature validation service server (SVS Serv) implements the SVA, which is the component of the service that implements the signature validation protocol (SPV) on the QSVSP's side. The application includes implementation of the validation algorithm defined in ETSI TS 119 1 02-1.

For this purpose, ZS allows for the service to call external factors, such as:

- the CA having issued the signer's certificate,
- status information services (OCSP) or
- certificate revocation lists (CRL),
- CA of the TSA that have provided timestamps,
- other QSVSP for complementary checks,
- trusted lists of EU member states,
- the trusted list of the European Commission, etc.

SVA builds the signature validation response based on validation algorithm, which includes:

- format verification,
- identification of the signer's certificate,
- validation context,
- X.509 validation,
- cryptographic validation,
- acceptance of the signature (i.e. the signature validation requirements), etc.



The signature / validation applications (VA) of ZS can be configured to operate on ZS server (through Internet connection to the Signature Validation Service (SVS Serv) server).

- Requests a signature validation to the signature validation service server (SVSServ);
- It is possible to request the validation of multiple signatures in accordance with ETSI TS 119 442;
- Executes the signature validation protocol (SVP) on the user's side;
- When applicable, takes care of the validation report presentation;

The client can incorporate:

- A user interface for manual input of the request; or
- A machine interface for automated requests; The request should be incorporated in 3rd party application (e.g. Zipper RepoLTA archiving application)
- A user interface to present the report.

- The validation report should contain Zipper Services qualified timestamp which is in line with Regulation (EU) No. 910/2014;
- The applicability checking, i.e. the final decision to "accept" a signature/seal on the basis of the validation report can be done by the user (manually), or by the client or the server (depending on the SVS implementation). This can be done according to signatures applicability rules that are specified in ETSI TS 119 172-1;
- In case of multiple signatures/seals on the same report the client application (DA) will use the result of validation of those signatures/seals and will interpret the result depending on the business context in which it is applied. Also, will allow to select, if necesarry, the specific signature to be verified in the case the verified content contains multiple signatures.

NOTE: The present document does not put requirements on the client. Only the DA's elements implemented on the server side are subject to requirements.

10. DEFINITIONS AND ABBREVIATIONS

10.1. DEFINITIONS

The terms and definitions given in ETSI EN 319 401 and ETSI TR 119 001 are applied, as well as the following ones:

applicability checking - determination whether a signature conforms to signature applicability rules. The applicability checking complements the signature validation service.

(signature) commitment type - the implication of the signature;

(signature) creation constraint - criteria used when creating a digital signature;

DSS(Digital Signature Service) - is an open-source software library, aimed at providing implementation of the standards for Advanced Electronic Signature creation, augmentation and validation in line with European legislation and the eIDAS Regulation in particular.

driving application (DA) - an application that uses a signature creation system to create or validate a signature. In the signature validation process, the application provides AdES digital signature and other input data to a signature validation application (SVA);

qualified validation service for qualified electronic signatures - as specified in Art. 33 of Regulation (EU) No. 910/2014;

qualified validation service for qualified electronic seals - as specified in Art. 40 of Regulation (EU) No. 910/2014;

qualified validation service provider (QSVSP) - a service provider that provides qualified validation service for qualified electronic signatures/seals validation;

signature acceptance - a technical process defined in ETSI TS 119 102-1 which constitutes part of the signature validation process. It is performed by submitting a signature validation application;

signature applicability rules - a set of rules applicable to one or more digital signatures that define the requirements for determination of whether a signature is fit for a particular business or legal purpose. These rules include signature validation policies containing validation constraints. ETSI TS 119 172-1 is applied for these purposes.

signature class - a set of signatures achieving a given functionality (e.g. a signature with time, a signature for long-term validation, etc.).

signature creation device - configured software or hardware used for the creation of an electronic signature;

signature validation application (SVA) - an application that validates a signature against a signature validation policy, and that outputs an indication of the signature validation status and a signature validation report. The signature validation application is specified in ETSI TS 119 1 021;

signature validation client (SVC) - a component or piece of software that implements the signature validation protocol on the user's side;

signature validation policy - a set of signature validation constraints processed or to be

processed by the SVA. The signature validation policy is a purely technical concept. The signature validation policy defines the signature applicability rules;

signature validation report (SVR) - a comprehensive report of the validation provided by the signature validation application to the DA and allowing the driving application and any party beyond the driving application to inspect details taken during the validation and investigate the detailed causes for the status indication provided to the signature. The report may be in line with ETSI TS 119 1 02-2 and the minimum requirements for its content are defined in clause 5.1.3 of ETSI TS 119 102-1;

Signature Validation Service (SVS) Policy - this is a set of rules that indicate the quality and the applicability of a signature validation service. The document determines the service applicability to a particular community and/or class of application with common security requirements. The SVS policy is applicable to a trust service as defined in ETSI EN 31 9 401;

signature validation service (SVS) practice statement - this is a statement of the practices and procedures used to address all the requirements identified for the provision of the signature validation service. The practice statement applies to a trust service that is part of the QSVSP's documentation in line with ETSI EN 319 401;

signature validation service server - a component that implements the signature validation protocol and processes the signature validation on the QSVSP's side;

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

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

signature verification - a process of checking the cryptographic value of a signature using signature verification data;

signer - an entity being the creator of a digital signature;

signature validation constraint - technical criteria against which a digital signature can be validated, as specified in ETSI TS 119 1 02-1;

user - an application or a human being interacting with the signature validation application;

validation - the process of verifying and confirming that an electronic signature or seal is valid;

validation data - data that is used to validate an electronic signature or an electronic seal;

validation of a qualified electronic signature - as specified in Art. 32 of Regulation (EU) No. 910/2014;

validation of qualified electronic seals - as specified in Art. 40 of Regulation (EU) No. 910/2014;

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

verifier - an entity that wants to validate or verify a digital signature.

10.2 ABBREVIATIONS

The terms and definitions given in ETSI EN 319 401 and ETSI TR 119 001 are applied, as well as the following ones:
AdES -Advanced Electronic Signature
API Application Programming Interface
ASiC Associated Signature Containers
BB Building Block (DIGITAL)
CA Certificate authority
CAdES CMS Advanced Electronic Signatures
CMS Cryptographic Message Syntax
CRL Certificate Revocation List
CSP Cryptographic Service Provider
DA – Driving Application;
DER Distinguished Encoding Rules
DIGITAL EC DIGITAL Building Block
DSA Digital Signature Algorithm - an algorithm for public-key cryptography
DSS European Commission Digital Building Blocks Digital Signature Service
ESI Electronic Signatures and Infrastructures
ETSI European Telecommunications Standards Institute
EUPL European Union Public License
HSM Hardware Security Modules
OCSP Online Certificate Status Protocol
ODF Open Document Format

ODT Open Document Text
PAdES PDF Advanced Electronic Signatures
PMC The Internal Governance Body of TSP
PoE Proof of Existence**;**
PKCS Public Key Cryptographic Standards
PKCS#12 It defines a file format commonly used to store X.509 private key accompanying public key certificates, protected by symmetrical password
PKIX Internet X.509 Public Key Infrastructure
RSA Rivest Shamir Adleman - an algorithm for public-key cryptography
OVR - OveRall/General requirements applicable to more than 1 (one) component;
QES - Qualified Electronic Signature or Qualified Electronic Seal;
(Q)SCD - (Qualified) Signature Creation Device;
QSVSP - Qualified Signature Validation Service Provider;
SCA Signature Creation Application
SD - Signer's Document;
SDO - Signed Data Object;
SDR - Signed Document Representation;
SSCD Secure Signature-Creation Device
SVA – Signature/Seal Validation Application;
SVP – Signature/Seal Validation Protocol;
SVR – Signature/Seal Validation Report;
SVS – Signature/Seal Validation Service;
SVSServ – Signature/Seal Validation Service Server;
TL Trusted List
TSA Time Stamping Authority
TSL Trust-service Status List
TSP Trusted Service Provider
TST Time-Stamp Token
UCF Universal Container Format
XAdES XML Advanced Electronic Signatures
ZIP File format used for data compression and archiving
VPR – Signature/Seal Validation Process.

11. Policies and practices

The SVS Policy is integrated in this document and contains information on the service applicability. The service recipients may be natural persons or legal entities and relying parties. The policy provides information about the level of the service.

The identifier of this Certification Policy will only be changed if there are substantial changes that affect its applicability.

• OID Tree	
1.3.6.1.4.1.57570	Identification Number (OID) of Zipper Services SRL, registered to IANA
1.3.6.1.4.1.57570.4.2.1.1	Validation Service **Conforms to the ETSI TS 119 441 validation criteria**
1.3.6.1.4.1.57570.4.2.2.3	Qualified Validation Service **Conforms to the ETSI TS 119 441 qualified validation criteria**

4 (validation) .2 (qualified Signature validation service). X(Policy). Y(version)

This Validation Policy is permanently updated and published at https://pki.ca.ezipper.ro/repository/policies.php

Note: The validation report specifies the key and level of the validated electronic signature / seal. The trusting third party is responsible for determining its applicability to the commercial purpose and, therefore, its acceptance or rejection.

ZS ensures that it does not alter the object identifier of this document as well as the object identifiers of policies, practices and other referral documents in any circumstances. If there is an extension/update in policy and practice that will not affect previously issued certificates, ZS presents a new object identifier that covers the new certificates or extended/updated ones.

The signature validation service (QSVSP) is integrated in this document and has been developed, is applied and updated as specified in ETSI EN 31 9 401. The SVS Practice Statement describes how ZS implements the service and is owned by the QSVSP. The practice statement is accessible to auditors, users and relying parties. This document describes the method of fulfilment of the requirements that have been identified as necessary to maintain the high quality of the signature validation service.

12. CERTIFICATE USAGE AND APPLICABILITY ON THE VALIDATION SERVICE

ZS offers a service of qualified validation of electronic signatures and seals which allows relying parties to receive a report on the signature/seal validation process in an automated and reliable way.

The SV service may be combined with other services for enhancing the signature, in accordance with the protocol indicated in ETSI TS 119 442 which supports the order for enhancing the reliability of the signature with the validation service.

The SV report should be generated independently in XML format and encrypted to safeguard integrity. The encryption happens by applying a Long-Term Archival signature (LTA-level signature) with a qualified time stamp provider and guarantees that signatures and seals are generated and validated in compliance with European legislation (eIDAS).

Another solution that ZS implemented is the validation of given document's electronic signature before the document is approved for archiving. The document to be archived is packaged in a digital container together with the SV Report, as well as other metadata detailing the archiving process. In the next step the container is encrypted to safeguard integrity. The encryption happens by applying a Long-Term Archival signature (LTA-level signature) with a qualified time stamp provider and electronically timestamped over ZIPPER Qualified Time-Stamping Services. The container is created based on the Associated Signature Container (ASiC) baseline profile for the container and the CMS Advanced Electronic Signature (CAdES) for the encryption.

13. Trust Service management and operation

13.1. Security Management

ZS QSVP ensures that administrative and management procedures are applied which are adequate and correspond to recognized best practices.

ZIPPER performs all SV functions using trustworthy systems that meet the requirements of ZIPPER ISMS.

13.2. Asset Classification and Management

ZIPPER maintains an inventory of all assets and assigns a classification for the protection requirements to those assets consistent with the risk analysis.

13.3. Personnel Security

ZIPPER maintains appropriate personnel controls fulfilling security best practice and the requirements of relevant standards.
Managerial and operational personnel possess the appropriate skills and knowledge of SV, digital signatures and Trust Services as well as security procedures for personnel with security responsibilities, information security and risk assessment.
ZIPPER implements the Trusted Roles Policy for all those employees that have access to or control cryptographic operations. Trusted Persons and Roles include, but are not limited to:

- Cryptographic business operations personnel,
- Security personnel,
- System administration personnel,
- Designated engineering personnel, and
- Executives that are designated to manage infrastructural trustworthiness.

Prior to commencement of employment in a Trusted Role, ZIPPER conducts background checks which may include indicatively the following:

- Verification of identity
- Check of previous employment and professional reference;
- Confirmation of the highest or most relevant educational degree obtained;
- Verification that there is no criminal conviction;
- Check of financial records.

ZIPPER requires that personnel seeking to become Trusted Persons present proof of the requisite background,

qualifications, and experience needed to perform their prospective job responsibilities competently, as specified in the employment contract and job description, before they perform any operational or security functions.
Employment contracts signed by the employees include confidentiality provisions for information that comes to their knowledge in the course of their performance.
ZIPPER ensures that personnel have achieved trusted status and departmental approval has been given before such personnel are:

- Issued access devices and granted access to the required facilities;
- Issued electronic credentials to access and perform specific functions on SVA, or other IT systems.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with a dedicated account, and administrative commands are only available with explicit permission. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are locked as soon as possible when the role change dictates.

13.4. Physical and Environmental Security

ZIPPER QSVP implements the Physical Security Policy, which supports the security requirements of this SV Policy & Practice Statement.
ZIPPER QSVP operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.
ZIPPER also maintains Disaster Recovery facilities for its Signature Validation Services operations. ZIPPER's Disaster Recovery facilities are protected by multiple tiers of physical security comparable to those of ZIPPER's primary facility.
ZIPPER operations are protected using physical access controls making them accessible only to appropriately authorized individuals. Access to secure areas of buildings requires the use of an "access" card and/or and biometrics. Access card use is logged by the building security system.
Access card logs are reviewed on a regular basis.
ZIPPER's secure facilities are equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control temperature and relative humidity.

ZIPPER has taken reasonable precautions to minimize the impact of water exposure to its facilities, as well as to prevent and extinguish fires or other damaging exposure to flame or smoke.
All media containing production software and data, audit, archive, or backup information is stored within ZIPPER facilities or in secure off-site storage facilities with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.
ZIPPER securely stores all removable media and paper containing sensitive information related to its operations in secure containers. Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed prior to disposal.

13.5. Operations Management

ZIPPER QSVP ensures that the procedures, processes and infrastructure to comply with the operational management, procedural security requirements, system access management, trustworthy systems deployment and maintenance, business continuity management and incident handling as defined in ETSI EN 319 421.
The operations management procedures for the ZIPPER QSVP are incorporated within the overall ZIPPER internal operations management procedures.

13.6. Compromise of SV Services

In the event of compromising the server offering SV Service, ZIPPER will not issue signature validation until steps are taken to restore the server.

13.7. Signature Validation Service Termination

The SV Service is terminated:

- with a decision of ZIPPER's Board of Directors;
- with a decision of the authority exercising supervision over the Signature Validation Services;
- with a judicial decision;
- upon the liquidation or termination of ZIPPER's operations
- cessation due to a disaster or significant reason from which no satisfactory recovery is possible.

ZIPPER ensures that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation of ZIPPER's services, and in particular, it ensures the continued maintenance of information required to verify the correctness of the services.

13.8. Compliance with Legal Requirements

ZS, as QSVP applies the requirements specified in clause 7.13 of ETSI EN 31 9 401 in order to ensure compliance with the legal requirements:

- Guarantees that it operates in a legal and trustworthy manner;
- It provides evidence on how it meets the applicable legal requirements;
- The trust services provided and the end user products used in the provision of those services are made accessible for persons with disabilities, where possible;

Appropriate technical and organizational measures are undertaken against unauthorized or unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data. ZS guarantees that personal data are processed in accordance with Regulation (EU) No. 2016/679. In this respect, authentication for a service online concerns processing of only those identification data which are adequate, relevant and not excessive.

In addition, the following specific requirements are applied:

- QSVSP does not store the signer's document (SD) after processing when not necessary. If the validation service works in combination with a long-term preservation service (e.g. archiving service), such data may need to be kept, based on a contractual agreement.

The QSVSP has the overall responsibility for meeting the requirements defined above when some or all of its functionalities are undertaken by subcontractors.

The service is provided in accordance with the requirements for qualified validation of qualified electronic signatures set out in Regulation (EU) No. 91 0/2014 (eIDAS: Art. 32 and 33) and seals (eIDAS: Art. 40)

Article 32 — Requirements for the validation of Qualified Electronic Signatures

The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

-the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;	The qualified electronic signature validation process fulfills the EU requirements for qualified trust service provider and is complying with Annex I(REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES)
-the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;	The qualified electronic signature validation process fulfils the EU requirements for qualified trust service provider that issues qualified certificates for an electronic signature and for an electronic seal.
-the signature validation data corresponds to the data provided to the relying party;	This is guaranteed through the supported formats for electronic signature/seal.
-the unique set of data representing the signatory in the certificate is correctly provided to the relying party;	The service automatically creates a **validation report** which contains the data from the electronic signature/seal certificates used for signing the document which the service has duly validated.
-the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;	The pseudonym is written in a special attribute in the Subject field and this ensures that there is clear indication of this fact for the relying party.
-the electronic signature was created by a qualified electronic signature creation device;	The qualified electronic signature validation process fulfills the EU requirements to check whether the electronic signature was created by a qualified electronic signature creation device (SSCD for QSign/QSeal) takes place.
-the integrity of the signed data has not been compromised;	This is ensured through the methodology for verification and validation of electronically signed documents described in this policy.
-the requirements provided for in Article 26 were met at the time of signing.	The signature validation process fulfils the EU requirements to check the requirements of Article 26 (requirements for an Advanced Electronic Signature): -is uniquely linked to the signatory; -is capable of identifying the signatory; -is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and -is linked to the data signed therewith in such a way that any subsequent change in the data is detectable. These checks are performed for all formats supported by the service.

The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.	This is ensured through the methodology for verification and validation of electronically signed documents described in this policy and practice.

Article 33 — Qualified Validation Service for Qualified Electronic Signatures

A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who: - provides validation in compliance with Article 32(1); and allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.	Compliance with Article 32 is presented in preceding paragraph.
The Commission may, by means of implementing acts, establish reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	This is ensured through the methodology for verification and validation of electronically signed documents and through the process of receiving the validation report described in this policy.

Article 40 Validation and preservation of qualified electronic seals

Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.	The service also covers the validation of electronic seals within the meaning of Art. 40.

13.9. Record Concerning Signature Validation Services

ZIPPER QSVP ensures that all relevant information concerning the operations of the ZIPPER SV Services is recorded for a defined period, in particular for providing evidence for the purposes of legal proceedings. The following records are maintained:

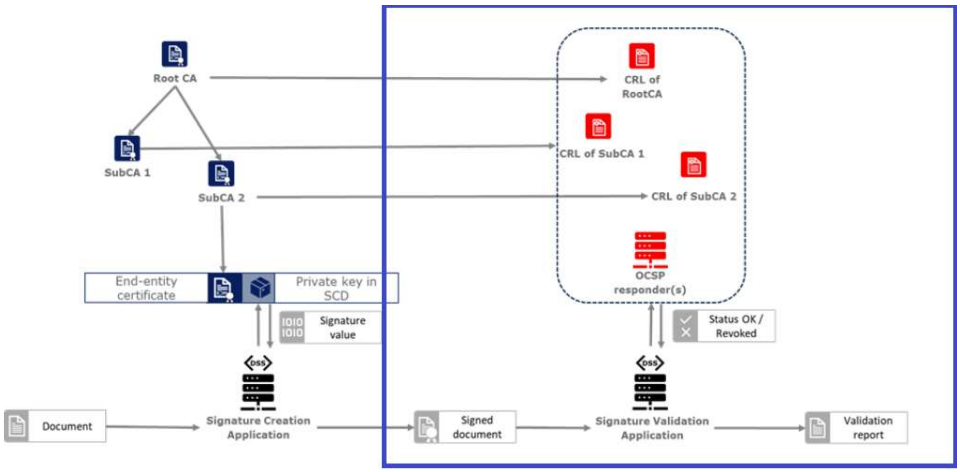
- SV requests with all pertinent information, forwarded by the applicant or collected electronically for the validation of the electronic signature or electronic seal, including at least the date and time of the validation of the qualified electronic signature or seal, the data provided by the applicant for the signature or seal validation (value of the electronic signature or of the electronic seal if the latter can be separated from the signed document or single representation of the signed document otherwise) as well as the identity of the applicant (IP from where access the service), the report containing the result of the validation of the qualified electronic signature or seal with the external data (trusted lists, EU LOTL, lists of revoked certificates, OCSP responses used to validate the signature or the seal.

13.10. Organizational reliability

ZIPPER TSA ensures that its organization is reliable as required in ETSI TS 119 441, art. 14.1. ZIPPER has the financial stability and resources required to operate in conformity with this TSA Policy & Practice Statement.

13.11. Signature validation service design

The standard ETSI EN 319 102-1 specifies a complete validation model and procedures for the validation of "AdES digital signatures", which are implemented in ZS SVA application.



The result of a validation process performed according to those procedures is a validation report and an indication which can be:

- TOTAL-PASSED indicating that the signature has passed verification and it complies with the signature validation policy.
- INDETERMINATE indicating that the format and digital signature verifications have not failed but there is insufficient information to determine if the electronic signature is valid.
- TOTAL_FAILED indicating that either the signature format is incorrect or that the digital signature value fails the verification.

In general, the validation of a signature is made against a set of constraints, which the cryptographic constraints are a part of, that is also sometimes referred to as a signature validation policy.

For each of the validation checks/constraint (e.g. signature format, signing certificate validity), the validation process must provide information justifying the reasons for the resulting status indication as a result of the check against the applicable constraints. In addition, the ETSI standard defines a consistent and accurate way for justifying statuses under a set of sub-indications. This allows the user to determine whether the signature validation has succeeded and the reason in case of a failure.

13.12. Supported Signature Formats

The SV application supports **signature formats**:

XAdES - for XML Advanced Electronic Signatures;

CAdES - for CMS Advanced Electronic Signatures;

PAdES - for PDF Advanced Electronic Signatures (cf. [R03]);

JAdES - for JSON Advanced Electronic Signatures (cf. [R05]);

ASIC - for Associated Signature Containers (ETSI EN 319 162) XAdES and CAdES combinations are possible.

Compliant with:

a) ETSI TS 103 171 (XAdES Baseline Profile);

b) ETSI TS 103 172 (PAdES Baseline Profile);

c) ETSI TS 103 173 (CAdES Baseline Profile);

d) ETSI TS 103 174 (ASiC Baseline Profile); and

e) ETSI standards on baseline profiles for CAdES digital signatures (ETSI EN 319 122-1), XAdES digital signatures (ETSI EN 319 132-1), and PAdES digital signatures (ETSI EN 319 142-1).

13.13. Implemented validation Processes

- ***Validation Process for Basic Signatures*** (-B)(see ETSI EN 319 102-1 clause 5.3): should be applied for signatures where the time of validation lies within the validity period of the signing certificate and the signing certificate has not been revoked.

- **Validation Process for Signatures with Time (-T) and Signatures with Long-Term Validation Material (-LT)** (see ETSI EN 319 102-1 clause 5.5). The SVA is able to use the validation data stored within the signature for validation.

- **Validation process for Signatures providing Long Term Availability and Integrity of Validation Material (-LTA)** (see ETSI EN 319 102-1 clause 5.6).

Rules:

- The validation process for Basic signature is executed against the first time which is the (current) validation time;

- The validation process for Signatures with Time and Signatures with Long-Term Validation Material is executed against a second time which is the "best signature time" that is determined using the signature timestamp;

- The validation process for Signatures with Archival Data is executed against a third time which is the "best signature time" determined using all time assertions present in the signature.

The overall validation result is provided as the indication returned by the validation process against which the validation was performed.

The SVA is compatible with the following basic profiles:

XAdES	CAdES	PAdES	JAdES
XAdES-B-B	CAdES-B-B	PAdES-B-B	JAdES-B-B
XAdES-B-T	CAdES-B-T	PAdES-B-T	JAdES-B-T
XAdES-B-LT	CAdES-B-LT	PAdES-B-LT	JAdES-B-LT
XAdES-B-LTA	CAdES-B-LTA	PAdES-B-LTA	JAdES-B-LTA

13.14. Validation Process Result

Depending on the format of electronic signature/seal used, the service supports validation processes for baseline formats of the signature/seal and advanced formats (with added electronic timestamp or time verification data) as follows (For a detailed description of their meaning, refer to ETSI EN 319 102-1):

Information entered in the report		**Semantics**
Indication	**Report data**	

TOTAL-PASSED	The validation process outputs the validated certificate chain, including the certificate for electronic signature/seal used in the validation process.	The qualified validation process of electronic signatures and seals results into TOTAL-PASSED based on the following considerations: • the cryptographic checks of the electronic signature/seal succeeded (including checks of hashes of individual data objects that have been signed indirectly); • any constraints applicable to the signer's identity certification have been positively validated (i.e. the signing certificate has been found trustworthy); and • the electronic signature/seal has been positively validated against the validation constraints and hence is considered conformant to these constraints.

TOTAL-FAILED	The validation process outputs additional information to explain the TOTAL-FAILED indication for each of the validation constraints that have been taken into account and for which a negative result occurred.	The qualified electronic signatures and seals validation process results into TOTAL-FAILED because the cryptographic checks of the electronic signature/seal failed (including checks of hashes of individual data objects that have been signed indirectly) or it has been proven that the generation of the signature/seal took place after its revocation.
INDETERMINATE	The validation process outputs additional information to explain the INDETERMINATE ation and to help the verifiers to identify what data is missing to complete the validation process.	The available information is insufficient for the validation process to ascertain the TOTAL-PASSED or TOTAL-FAILED status of the ronic signature/seal.

13.15. Signature validation process requirements

The implemented signature validation process follows the ETSI TS 119 102-1 algorithm.

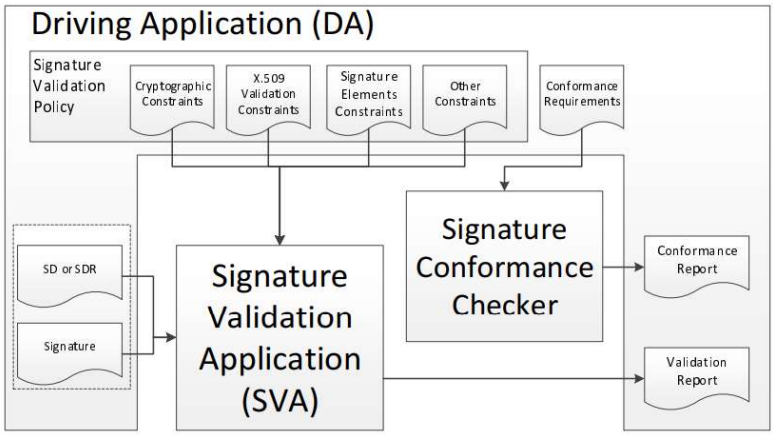


Fig. Conceptual Model of Validation

The standard defines the conceptual model by dividing software with signature validation functions into two parts:

- a signature validation application (SVA); and
- a driving application (DA).

The signature validation application (SVA) receives an AdES digital signature and other input from the driving application (DA). The SVA shall validate the signature against a signature validation policy, consisting of a set of validation constraints, and shall output a status indication and validation report providing the details of the technical validation of each of the applicable constraints, which can be relevant for the DA in interpreting the results.

ZS implemented DSS (European ComissionDigital-building-blocks Digital Signature Service) in internal infrastructure for SV Application. DA should represent different driving applications, implemented in ZS infrastructure (e.g. archiving application). The present document does not stipulate any required behavior by the DA, especially no processing requirements for any of the returned information, since this is application specific and out of the scope of the present document.

Based on SVA results:

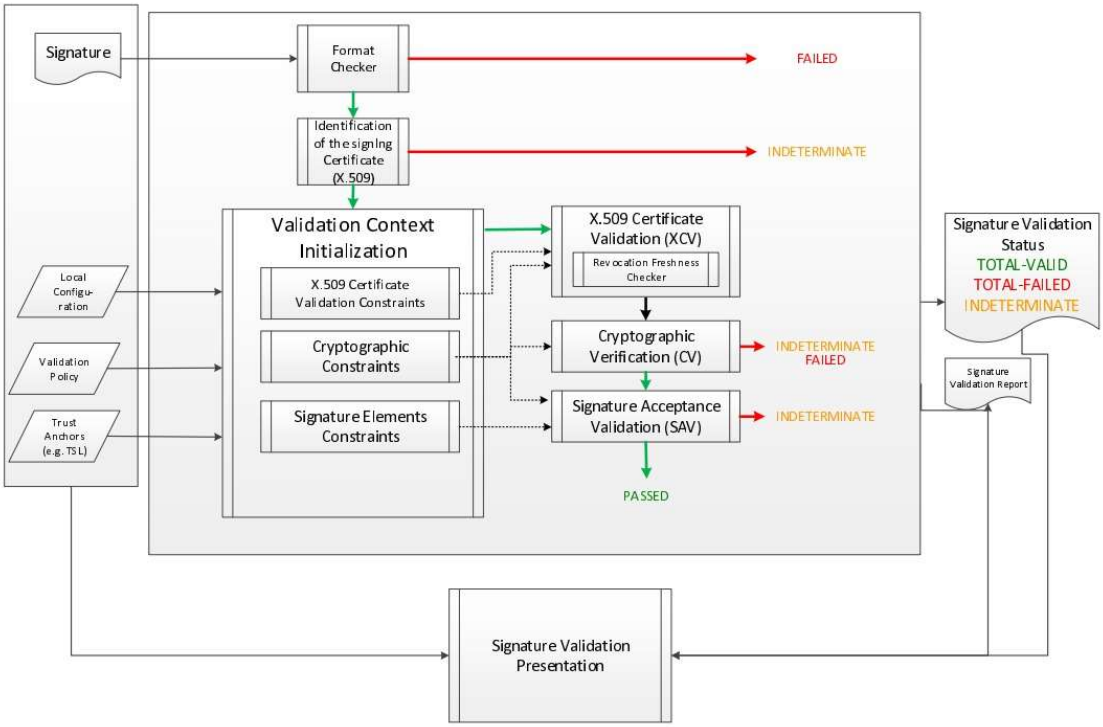
- If SVA returns TOTAL-PASSED for a certain signature, DA should consider the signature as a technically valid signature according to the validation constraints.
- If SVA returns TOTAL-FAILED, the DA should not consider the signature as technically valid.
- In case the SVA returns INDETERMINATE, if the subindication indicates the result can change when rerunning the algorithm, the DA may retry validation based on additional information or at a later point in time. In all other cases, the acceptation of the signature has to be determined by the DA, or beyond, by the user, as part of the applicability rules checking.

SVS is implemented, such as:

- as a web service;
- an independent a web application.

13.16. THE PROCESS OF SIGNATURE VALIDATION

The validation process is based on the ETSI standard EN 319 102-1. The simplified diagram below, shows the process of the signature validation, with the relationships between each building block which represents a logic set of checks used in validation process:



13.16.1. Certificate chain (path) validation

The signature validation starts from a validation of a certificate chain. The certificate path validation is an algorithm that seeks to verify the binding between the public key and the subject of a certificate, using trust anchor information. The complete processing is described in RFC 5280 section 6.1, and as stated there, it verifies among other things that a prospective certification path (a sequence of n certificates) satisfies the following conditions:

a. for all x in {1, …, n-1}, the subject of certificate x is the issuer of certificate x+1;
b. certificate 1 is issued by the trust anchor;
c. certificate n is the certificate to be validated (i.e., the target certificate); and
d. for all x in {1, …, n}, the certificate was valid at the time in question.

In ETSI EN 319 102-1, a prospective certificate chain is defined as a sequence of certificate that satisfies the conditions a. to c. above and for which the trust anchor is trusted according the validation policy in use.

In SV application, for a given certificate, the framework builds a certificate path until a known trust anchor (trusted list, keystore), validates each found certificate (OCSP / CRL) and determines its European "qualification".

13.16.2. Determine the certificate qualification

The framework follows the standard ETSI TS 119 615. It analyses the certificate properties (QCStatements, Certificate Policies, etc.) and applies possible overrules from the related trusted list.

SVA always computes the status at 2 different times: certificate issuance and signing/validation time. The certificate qualification can evolve in time, its status is not immutable (e.g.: a trust service provider can lose the granted status). The eIDAS regulation clearly defines these different times in the Article 32 and related Annex I.

When the signature validation service aims to validate qualified electronic signatures or seals as defined in Article 32.1 of Regulation (EU) No 910/2014, the validation process will follow the requirements of ETSI TS 119 172-4 (draft phase).

A signature can be determined as qualified if:

- The result of running the "validation process for Signatures providing Long Term Availability and Integrity of Validation Material" defined in ETSI EN 319 102-1 is TOTAL_PASSED;

- The signing certificate is determined as qualified at “best-signature-time” and at “issuance time” (the time when the certificate was issued i.e. the value of the "notBefore" field);

- The private key corresponding to the signing certificate is determined as being held in a qualified signature creation device (QSCD).

13.16.3. Verify Revocation

The revocation freshness constraint (RFC) is a time interval indicating that the validation accepts CRLs that were emitted at a point in time after the validation time minus the RFC: *valTime - RFC < CRL.thisUpdate*.

If the RFC is respected by a CRL then that CRL can be used. Otherwise, the CRL shall be rejected and shall not be used to determine whether the certificate is revoked or not. Another CRL can be searched online. If no CRL respecting the RFC is found, then it cannot be determined whether the certificate is valid, and it is thus not possible to determine whether the signature is valid.

- In case of a signature with a BASELINE-T level, the validation time can be replaced by the *best-signature-time* when checking the constraint. Revocation data should be issued after the best-signature-time, provided by a signature timestamp.
- In case of a BASELINE-B level, there is no timestamp among the unsigned attributes. If the RFC is equal to 0 then the validation time needs to be smaller than the *CRL.thisUpdate*. This means that the revocation data needs to have been issued after the validation process is concluded which is not possible.

According to the ETSI TS 119 172-4 standard, the RFC shall be set to 0 (zero). If DSS had had an RFC equal to 0 then it would invalidate all B-level signatures without a signature timestamp. Therefore, revocation freshness is not checked in SVA by default. The validation level of the check is set to IGNORE, meaning users are shown that the check exists, but it is not executed in the validation process.

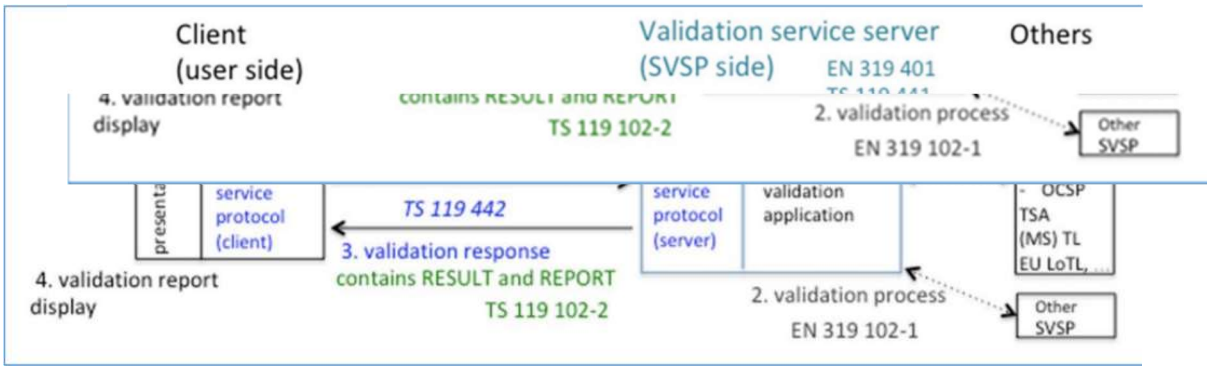
13.16.4. Access External Resources

In case of a signature with BASELINE-LT or BASELINE-LTA level the SVA will provide the following sources of information and parameters:

- the source of trusted certificates (based on the trusted list(s) specific to the context);
- the source of intermediate certificates used to build the certificate chain until the trust anchor. This source is only needed when these certificates are not included in the signature itself;
- the source of AIA;
- the source of OCSP;
- the source of CRL;

13.16.5. Functional Procedure of the Validation Service:

Step 1	(DA) generates and sends a signature validation request to SVA. The protocols supporting the request and the response correspond to the ETSI TS 119 442 specification. The request includes: 1. The signed document (s) (SD) and the signature (s) (SDO (s)) that signs them; or 2. the signed document (s) representation (s) (SDR (s)) and the signatures that sign them, to avoid exposing the content of the document to the validation service. Mapping between signed documents and their summaries used within signatures is essential when verifying a signature. In accordance with Regulation (EU) No. 910/2014, 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 send only the hashed summaries of signed documents. In this case, the verification of the integrity of the signed document and its correspondence with the signature is beyond the control and responsibility of the SVA.
Step 2	validation process corresponds to the ETSI TS 119 102-1 specification. Validation is performed by the SVA in accordance with this signature validation policy. The signature of the validation process follows the provisions of ETSI TS 119 102-1.
Step 3	The protocols that support the request and the response are those specified in ETSI TS 119 442. e validation response includes the validation reports. It includes the OID of the Service Policy and the OID of the signature validation policy used. The validation report corresponds to the ETSI TS 119 102-
Step 4	The DA can offer a signature validation presentation module to present the validation report that specifies the result and provides detailed report of each of the signed attributes. The DA, under his



13.16.6. Signature Validation Report Requirements

- The validation report may be provided to the relying party automatically in accordance with **ETSI TS 119 442** and **ETSI TS 119 102-2**;

- The standard **ETSI EN 319 102-1** specifies a complete validation model and procedures for the validation of "AdES /QC digital signatures". The validation report will contain the result of a validation process performed according to those procedures is a validation report and an indication which can be:
    - ***TOTAL-PASSED*** indicating that the signature has passed verification and it complies with the signature validation policy.
    - ***INDETERMINATE*** indicating that the format and digital signature verifications have not failed but there is insufficient information to determine if the electronic signature is valid.
    - ***TOTAL_FAILED*** indicating that either the signature format is incorrect or that the digital signature value fails the verification.

- The validation report should be presented to the user through a web page within a TLS session supported by a certificate issued by the certification authority in a form convenient for them;

- The signature (OID) validation policy is in line with ETSI TS 119 172-4 and unambiguously states that the signature is qualified according to Regulation (EU) No. 910/2014;

- The validation report allows the relying party to be confident in the security of the signature/seal. There is information that:
    - the certificate has been issued by a Qualified Trust Service Provider and that it has been valid as of the moment of being signed
    - The data about the signature validation correspond to the data provided by the relying party.
    - The use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing.
    - The electronic seal is created by an electronic sealing device.
    - The integrity of the data signed is not threatened.

The SV provides a validation report in PDF and/or XML format

Structure and semantics of the Validation report

Main indication	Sub-indication	Report data	Semantics
TOTAL-FAILED	FORMAT_FAILURE	The validation process provides the individual facts that have resulted in information	The electronic signature/seal is not compatible with the standards supported specified in
	HASH_FAILURE	The signature validation process provides an identifier that uniquely identifies the element within the signed data object/seal causing the failure in the form of the certificate for electronic signature/seal.	The qualified validation process of electronic signatures and seals results into TOTAL-FAILED because at least one hash of a signed data object that has been included in the signing process does not match the
	SIG_CRYPTO_FAILURE	The validation process outputs the certificate for electronic signature/seal used in the validation process. The value of the signature cannot be verified with the help of the public key of the signature/seal.	The qualified validation process of electronic signatures and seals results into TOTAL-FAILED because the digital value of the signature could not be verified using the signer's public key in the certificate for electronic signature/seal.
	REVOKED	The validation process provides the following: - The certificate chain used in the validation process; - The time and, if available, the reason of revocation of the certificate for electronic signature/seal. - CRL, if any, for which the	The qualified validation process of electronic signatures and seals results into a TOTAL-FAILED because: - the certificate for electronic signature/seal has been revoked; and - there is proof of existence (PoE) available that the time of the
	SIG_CONSTRAINTS_FAILURE	The validation process provides multiple reasons that have resulted in unsuccessful validation.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because one or more attributes of the electronic signature/seal do not match the validation constraints.
	CHAIN_CONSTRAINTS_FAILURE	The validation process provides the following: - The certificate chain used in the validation process. - Additional information on the cause that has led to this result.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the certificate chain used in the validation process does not match the validation constraints related to the certificate. Additional information on the

			cause that has led to this result
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The validation process provides additional information on the reason for this result.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the validation of the certificate chain has produced an error for an unstated/unspecified reason.
	CRYPTO_CONSTRAINTS_FAILURE	The validation process provides identification of an electronic signature/seal or of a certificate generated using an algorithm or key size below the required cryptographic security level.	Keys used with such algorithms, are below the required cryptographic security level, and: • the electronic signature/seal and/or the corresponding certificates have been produced after the time up to which these algorithms/keys were considered secure (if such a time is known); and • the electronic signature/seal is not protected by a sufficiently strong timestamp applied before the time up to which the algorithm/key was considered secure (if such a time is known). Algorithms and keys accepted over the years are mentioned in constrains.xml)
INDETERMINATE	EXPIRED	The validation process provides data about the validated certificate chain.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because time of placing the electronic signature/seal is after the expiration date (notAfter) of the certificate.
	NOT_YET_VALID	The validation process provides data about the validated certificate chain.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because time of placing the electronic signature/seal lies before the expiration date (notBefore) of the certificate.

POLICY_PROCESSING_ERROR	The validation process provides additional information on the reason.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the given formal policy file could not be processed for any reason (e.g. not accessible, not pursuable, digest mismatch.
SIGNATURE_POLICY_NOT_AVAILABLE	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the document containing the details of the policy is not
TIMESTAMP_ORDER_FAILURE	The validation process outputs a list of timestamps that do no respect the ordering constraints.	The qualified validation process of electronic signatures and seals results into INDETERMINATE the provided list of timestamps and/or signed data object(s) do not respect the constraints on the order.
NO_SIGNING_CERTIFICATE_FOUND	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the certificate for electronic signature/seal cannot be identified.
NO_CERTIFICATE_CHAIN_FOUND		The qualified validation process of electronic signatures and seals results into INDETERMINATE because no certificate chain has been found for the identified certificate for electronic signature/seal.
REVOKED_ NO_POE	The validation process provides the following: •The certificate chain used in the validation process. • The time and the reason of revocation of the certificate for electronic signature/seal.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the corresponding certificates has been revoked during the validation. However, it may not be established whether the signature time lies before or after the revocation time.
REVOKED_CA_NO_POE	The validation process provides the following: •The certificate chain which includes the revoked certification authority certificate; • The time and the reason of revocation of the certificate.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because at least one certificate chain was found but an intermediate certification authority is revoked.

OUT_OF_BOUNDS_NO_POE		The qualified validation process of electronic signatures and seals results into INDETERMINATE because the certificate is expired or not yet valid at the validation date/time and the SVA cannot ascertain that the signing time lies within the validity interval of the certificate.
CRYPTO_CONSTRAINTS_FAILURE_NO_POE	The validation process provides the following: Identification of the electronic signature/seal or the respective certificate that is produced using an unacceptable key size or algorithm that does not meet the required cryptographic security level.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because at least one of the algorithms that have been used in the electronic signature/seal or the respective certificates involved in their validation, or the size of a key used with such an algorithm, is below the required cryptographic security level, and there is no proof that the signature/seal or these certificates were produced before the time up to which this algorithm/key was considered secure.
NO_POE	The validation process only identifies signatures/seals for which the proof of existence (PoEs) are missing. The validation process should provide additional information about the problem.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because there is no proof of existence (PoE) to ascertain that the signature/seal has been produced before some known compromising event (e.g. broken algorithm).
TRY_LATER		The qualified validation process of electronic signatures and seals results into INDETERMINATE because not all constraints can be fulfilled using available information. However, the process may be possible if the validation uses additional revocation information that will be available at a later point of time.

	SIGNED_DATA_NOT_FOUND	The validation process provides the following: The identifier (e.g. an URI) of the signature/seal data that caused the failure.	The qualified validation process The qualified validation process of electronic signatures and seals results into INDETERMINATE because the data about the signature/seal cannot be obtained.
	GENERIC	The validation process provides additional information showing why the validation indication is	The qualified validation process results into INDETERMINATE because of other reasons.

The Validation report is a representation of steps performed during the validation process, as defined in the ETSI EN 319 102-1 standard, and structured using the processes and blocks defined in that standard:

- Basic Building Blocks;
  - **FC** - Format Checking;
  - **ISC** - Identification of the Signing Certificate;
  - **VCI** - Validation Context Initialization;
  - **RFC** - Revocation Freshness Checker;
  - **XCV** - X.509 certificate validation;
  - **CV** - Cryptographic Verification;
  - **SAV** - Signature Acceptance Validation.
- Validation Process for Basic Signatures;
- Time-stamp validation building block;
- 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.
- For example the Basic Building Blocks are divided into seven elements:

The following additional elements also can be executed in case of validation in the past:

- PCV **- Past Certificate Validation;**
- VTS **- Validation Time Sliding process;**
- POE extraction **- Proof Of Existence extraction;**
- PSV **- Past Signature Validation.**

To process the revocation data, SVA performs the following additional checks:

- **CRS** (CertificateRevocationSelector) - validates a set of revocation data for a given certificate and returns the latest valid entry known to contain information about the concerned certificate;
- **RAC** (RevocationAcceptanceCheck) - verifies whether one single revocation data is known to contain information about the concerned certificate.

constraints

13.17. Cryptographic algorithm constraints

13.17.1. X.509 validation constraints

- The signer certificate's Key Usage field must have nonRepudiation bit set (also referred to as contentCommitment).

13.17.2. Hash algorithm constraints:

- In case of BDOC format: when validating a signature where SHA-1 function has been used then a validation warning about weak digest method is returned.

13.17.3. Asymmetric cryptographic algorithm contraints:

- RSA and ECC cryptographic algorithms are supported
- In case of PAdES/XAdES(also BDOC)/CAdES formats, the RSA key lenght must be at least 1024 bits and ECC key length at least 192 bits.
  - <Algo Size="160">DSA</Algo>
  - <Algo Size="1024">RSA</Algo>
  - <Algo Size="160">ECDSA</Algo>
  - <Algo Size="160">PLAIN-ECDSA</Algo>

13.17.4. Trust anchor constraints

1. The signature must contain the certificate of the trust anchor and all certificates necessary for the signature validator to build a certification path up to the trust anchor. This applies to the signer's certificate and the certificates of trust service providers that have issued the time-stamp token and revocation data that are incorporated in the signature.
2. Trust Anchors are:
   - In case of XAdES/CAdES/PAdES formats: EU Member State Trusted Lists.

13.17.5. Revocation data constraints

1. The signature must contain evidence record to confirm that certificate was valid at the time of signing.
2. The evidence record of signer certificate must be in the form of an OCSP confirmation or as a Certificate Revocation List.
3. No additional revocation data other than the data that was originally incorporated in the signature shall be requested during validation time.
4. Checking revocation of certificates regarded as Trust Anchors:

- In case of XAdES/CAdES/PAdES formats: revocation of Trust Anchor certificates is checked on the basis of the data in Trusted Lists.

13.17.6. Signer certificate's revocation freshness constraints

1. In case of XAdES/CAdES/PAdES BASELINE_LT and BASELINE_LTA signatures with signature time-stamp: revocation data freshness is checked according to the following rules:
   - In case of OCSP responce if difference between signature time-stamp's production time (genTime field) and signer certificate OCSP confirmation’s production time (producedAt field) is more than 24 hours then the signature is considered invalid. If the difference is more than 15 minutes and less then 24h then a validation warning is returned.
   - In case of Certificate Revocation List the signature time-stamp's production time (genTime field) must be within validity range of the CRL (between thisUpdate and nextUpdate)

13.17.7. Trusted signing time constraints

1. Trusted signing time, denoting the earliest time when it can be trusted (because proven by some Proof-of-Existence present in the signature) that a signature has existed, is determined as follows:
   - In case of signature with time-stamp (BASELINE_T, BASELINE_LT or BASELINE_LTA level) - the genTime value of the earliest valid signature time-stamp token in the signature.
   - In case of basic signature (BASELINE_B) - the trusted signing time value cannot be determined as there is no Proof-of-Existence of the signature.

13.17.8. ASICE container specific requirements

The ASICE container must conform with ETSI EN 319 162-1 standard. 1. Warning is returned when signatures in the container do not sign all of the data files. 2. Manifest file must be present.

13.17.9. ASICS container specific requirements

The service supports both signature and Time Stamp Token (TST) based ASIC-S containers. Evidence record based containers are not supported. The ASIC-S container must conform with ETSI EN 319 162-1 and ETSI EN 319 162-2 standards.

1. Manifest file can not be present in case of signature based ASIC-S containers.
2. Only one TimeStampToken per container is supported. No AsicArchiveManifest.xml support.
3. No TSL based verification of certificates is done in case of TimeStampToken based containers.