certSIGN Paperless Validation Policies and Practices Statement

for

Qualified Signature/Seal Validation Service

QSVS-PPS-EN

Version/Date: v1.7 – 31 Mar.2026

Important Notice

Address: 29 A Tudor Vladimirescu Avenue,
AFI Tech Park 1, Bucharest, Romania
Phone: 004-021-31.19.901

Web: www.certsign.ro

Document History

Version	Effective Date (last day of the month)	Reason	The person who made the change
0.1	July 2021	First version publishing	PKI Policies Manager
1.0	July 2022	Updates in content	PKI Policies Manager
1.1	August 2022	Minor updates after audit	PKI Policies Manager
1.2	January 2023	Annual review	PKI Policies Manager
1.3	January 2024	Annual review	PKI Policies Manager
1.4	March 2024	Appendix 3 added in full	PKI Policies Manager
1.5	15 January 2025	Annual review	PKI Policies Manager
1.6	15 January 2026	Annual review	PKI Policies Manager
1.7	31 March 2026	eIDAS2 updates	PKI Policies Manager

This document was created and is the property of:

Owner	Author	Date created
BU eIDAS Trusted Services	PKI Policies Manager	July 2021

Distribution List

Destination	Date distributed
Public-Internet	July 2022
Public-Internet	August 2022
Public-Internet	January 2023
Public-Internet	January 2024
Public-Internet	March 2024
Public-Internet	January 2025
Public-Internet	January 2026
Public-Internet	March 2026

This document was approved by:

Version	Name	Date
1.0	Policies and Procedures Management Body	July 2022
1.1	Policies and Procedures Management Body	August 2022
1.2	Policies and Procedures Management Body	January 2023
1.3	Policies and Procedures Management Body	January 2024
1.4	Policies and Procedures Management Body	March 2024
1.5	Policies and Procedures Management Body	January 2025
1.6	Policies and Procedures Management Body	January 2026
1.7	Policies and Procedures Management Body	March 2026

Table of Content

1 Introduction

1.1 Overview

This document, **certSIGN Paperless Validation, Policies and Practices Statement for Qualified Signature/Seal Validation Services** (QSVS-PPS-EN), describes the policies and practices applied by Certsign S.A. (certSIGN) in providing the Qualified Signature/Seal Validation Services in conformity with:

• Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

• Legal acts of Romania (like Law 214/2024, Order 449/2017);

• EU standard ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

• ETSI TS 119 441 V1.2.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.

The structure of this document is compliant to Annex A of ETSI TS 119 441.

1.1.1 TSP identification

S.C. CERTSIGN S.A.
Office: 29 A, Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania
Trade Register Number: J2006000484402
Tax registration code: RO 18288250
Registered office: 107A Oltenitei Street. building C1, Fl.1, room 16, District 4, Bucharest, Romania, PC 041303

1.1.2 Supported signature validation service policies

The Qualified Signature/Seal Validation Service (QSVS) policy is dedicated to the validation of qualified signatures and/or qualified seals according to the EU Regulation.
The main policy limitation is on the validation of signatures or seals placed on pdf documents. Only one document can be validated at a time.
certSIGN as a QSVSP is conform to ETSI TS 119 441 requirements and use the following specific OID: **0.4.0.19441.1.2**

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

The document is validated if it was not changed since the last signature/seal on it and if all the signatures/seals are valid and qualified according to the EU Regulation no 910/2014.

Signature-policy-compliance - It indicates that the processing for validating the digital signature and generating the corresponding applicability rules checking report complies with the requirements of the ETSI TS 119 172-4.

- id-etsi-sars-SpCompliance - **0.4.0.191724.1.1**

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

certSIGN Signature Validation policies

• 1.3.6.1.4.1.25017 (certSIGN organization).4 (Validation).2 (Qualified Signature Validation Service).X (policy).Y (version)

- Default – PadES validation policy - OID: 1.3.6.1.4.1.25017.4.2.1.2
- CAdES validation policy - OID: 1.3.6.1.4.1.25017.4.2.2.1

The specific validation policies statement summaries are presented in Appendix 2.

1.2 Signature Validation Service Components

1.2.1 SVS actors

The QSVS-PPS regulates the most important relations between entities belonging to certSIGN, advisory teams (including auditors) and customers (users of the services provided) of this:

- certSIGN Certification Authorities (CAs)
- Repository,
- Online Certificate Status Protocol (OCSP Authority),
- Certificates Revocation Lists (CRL Authority)
- Time Stamp Servers (TSA Authorities)
- Subscribers,
- Relying Parties,
- Policies and Procedures Management Body
- Auditors

1.2.2 Service architecture

The diagram below displays the simplified certSIGN Qualified Validation Service architecture and the involved actors.

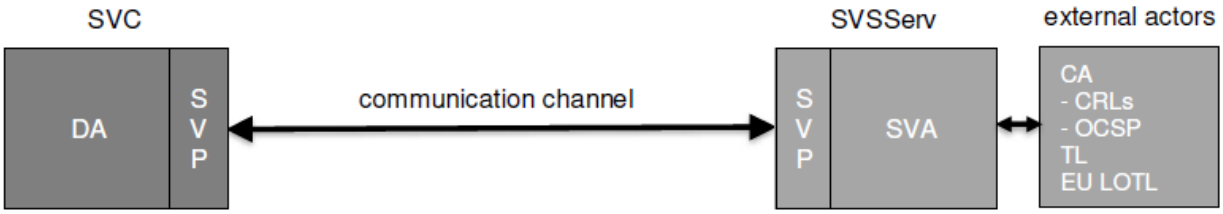


Figure 1 Service architecture

The **Signature Validation Client** (SVC):

- executes the **Service Validation Protocol** (SVP) on the user's side
- builds the signature validation request
- present or send the validation report

The **Signature Validation Service Server** (SVSServ):

- executes the SVP and processes the signature validation on the SVSS side
- runs the **Signature Validation** Application (SVA) that:
  - implements the validation algorithm
  - call external actors to fulfill its purpose
- creates the **Signature Validation Report** (SVR) related to the request
- builds the signature validation response and return it to the SVC

1.2.3 Essential Policy requirements

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.

the certSIGN Validation Service can generally be called by an APP in a Fully Delegated Mode, with the entire signed data (SD) being sent.

Due to the fact that subsequently specified rules may appear quite complex to non-technical readers/stakeholders of the present policy document, the remaining part of the present overview provides an informal, non-normative summary of the essential policy requirements:

P1. The present policy document specifies validation rules for electronic signatures and seals that conform to the ETSI standards for Qualified Electronic Signatures, in particular to PAdES.

P2. Although an individual policy may be defined for each supported signature format and validation mode for the purpose of appropriately addressing signature format-specific details and mode-depending responsibilities of the involved actors, namely CertSIGN and the APP that has a validation service contract with CertSIGN, the overall set of validation rules is common for all policies of the present document. The default supported formats are the ones specified in ETSI EN 319 142-1.

P3. In the fully validation mode, the service receives the entire document from the business application, in particular a PDF document in the case of a PAdES-specific policy and is consequently enabled to specifically validate whether a hash calculated over signed content matches with the hash in the corresponding signed data object. The input document is instantly deleted after validation. The validation report is kept 3 years.

P4. In any case, the business application must enable relying party end-user to visualize signed parts/versions of a document in order to verify whether the signed content matches with the user's expectations so that the right decisions can be taken and that prevention of fraud is better addressed.

P5. The validation service validates all signatures and seals pertaining to the same input document and supplies resulting diagnostics in a single report. It does however not make any interpretation of supplied diagnostics or mutual relationship of those signatures and seals.

P6. The validation algorithm conforms to ETSI TS 119 102-1 – "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation". It uses the shell model for certificate validation as specified in section 5.2.6 of that standard. The algorithm only uses trust anchors that are published in the EU Trusted Lists.

P7. The validation algorithm only accepts trusted and qualified timestamps as proofs of existence of data that are used during validation. During this process, any expired or obsolete elements are not taken into account. In particular, expiration can also concern cryptographic algorithms when they do not conform to the requirements specified in ETSI TS 119 312 – "Electronic Signatures and Infrastructures (ESI); Cryptographic suites", for the point of time for which they are required to be resilient.

The validation algorithm always takes all eligible elements contained in a signed data object into account for performing a *Validation for Signatures* based on the actually existing profile of a given signature as specified in section 5.1.2 of ETSI TS 119 102-1 – "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

P8. The validation algorithm verifies and determines signed attributes contained in a signed data object, in particular signature policy and commitment type indications. It does however not interpret those elements and leaves it up to the discretion of the business applications as to whether those elements are used for taking further business decisions.

P9. The validation service does not allow the user to select the certificate(s) to be used for the validation, e.g. for the case where attributes of the SDO do not contain the certificate(s) needed. It allows only the implicit signature validation policy to be used amongst the available ones – for PaDES.

P10. The validation service allows the user to provide some inputs for the validation process (i.e. elements to parameterize the validation policy such as the signature class, but not a trust anchor).

certSIGN management is responsible for the implementation of the best practices required in order to fulfill all the validation policies from the current document.

In any case in which the certSIGN liability is incurred, it shall be limited to the value of the contract at the date of the damage.
certSIGN Paperless Validation service event logs are retained for 3 years;
Disputes related to Trust Services provided by certSIGN shall be settled initially through a conciliation procedure, (*https://www.certsign.ro/en/procedure-receiving-procesing-complaints/*) during which both Parties shall in good faith negotiate solutions in respect of any disputes arising. If the specific complaint is not settled within thirty (30) days of the commencement of the conciliatory process, the Parties may refer the dispute to the appropriate courts of Bucharest, Romania (the applicable legal system).
The TSP's trust service conformity assessment scheme is based on the LSTI-Q055-v6.4 scheme, referencing ETSI EN 319 401 and ETSI TS 119 441.

Availability of certSIGN document repository and the combined CRL repository is designed to exceed 99.8% of business hours - defined as 24 hours a day, seven days a week, excluding planned maintenance periods. Planned maintenance periods will be announced on https://www.certsign.ro at least 24 hours in advance.

In case of unavailability due to a catastrophe, failure of infrastructure outside the control of certSIGN or any other reason, certSIGN will make best endeavours to reinstate availability of the service within 24 hours.

1.3 Definitions and abbreviations

1.3.1 Definitions

Certification Authority - Trust Service Provider that issues certificates for electronic signatures and/or seals.
eIDAS Regulation - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Trust Service Provider - An entity which provides al least a Trust Service granted by the Supervisory Body.
Qualified Signature Validation Service – A Qualified Trust Service for Signature and/or Seal Validation
Qualified Trust Service Provider - An entity which provides al least a Qualified Trust Service granted by the Supervisory Body.
Qualified Validation Service - A Qualified Trust Service for Signature and/or Seal Validation, when applied on a digital document
Relying Party - A natural or legal person that relies on Trust Service
Signature Validation Practice Statement - A statement of the practices that certSIGN employs in providing its Trust Service for Signatures Validation.
Signature Validation Service - Trust Service for Signature and/or Seal Validation
Subscriber - A legal or natural person bound by an agreement with certSIGN to specific Subscriber obligations
Supervisory Body - The authority that is designated by a member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state.

1.3.2 Abbreviations

AdES	Advanced Electronic Signature
AdES/QC	Advanced Electronic Signature created with a Qualified Certificate
CA	Certificate Authority
CRL	Certificate Revocation List
CMS	Cryptographic Message Syntax
DTBS	Data to Be Signed or Data Been Signed Comprises the SD and additional attributes for being signed or being validated
ESI	Electronic Signatures and Infrastructures
LOTL	List Of Trusted Lists
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PoE	Proof of Existence
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
SVA	Signature Validation Application
SVP	Signature Validation Protocol
SVR	Signature Validation Report
SVS	Signature Validation Service
SVSP	Signature Validation Service Provider
TSP	Trust Service Provider
XML	eXtensible Markup Language

1.4 Policies and practices

certSIGN TSP carry out an yearly updated risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues. Then it selects the appropriate risk treatment measures, taking account of the risk assessment results.The risk treatment measures ensure that the level of security is commensurate to the degree of risk.

certSIGN TSP determined all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the certSIGN Information Security Policy and the Risk Management internal documents. The risk assessment is regularly reviewed, revised and approved by certSIGN management who accepts the residual risk identified.

The practices presented in this document are sustained by internal operational procedures and/or instructions for each phase of the TSP management and operations presented in Chapter 2. certSIGN has a review process for the practices including responsibilities for maintaining the TSP's practice statement.

1.4.1 Organization administrating the TSP documentation

The present document is administered by the certSIGN Trust Service Provider (TSP) through the Policies and Procedures Management Body (PPMB). The PPMB includes senior members of the management as well as staff responsible for the operational management of the certSIGN TSP PKI environment.

Name	S.C. CERTSIGN S.A. Office: 29 A Tudor Vladimirescu Avenue, AFI Tech Park 1, Bucharest, Romania Trade Register Number: J2006000484402 Tax registration code: RO 18288250 Registered office: 107A Oltenitei Street. building C1, Fl.1, room 16, District 4, Bucharest, Romania, PC 041303
Phone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table 1 Organization administering the document

Name	Policies and Procedures Management Body
Phone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table 2 Person determining the suitability for the policy

1.4.2 Contact person

The contact person for the updating of this document is the PKI Policies Manager of certSIGN. The contact person for the management and approval of this document is PPMB:

Name	Policies and Procedures Management Body (PPMB)
Phone	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table 3 Contact person

1.4.3 TSP (public) documentation applicability

The **Qualified Signature/Seal Validation Services Policies and Practices Statement** (QSVS-PPS) describes the policies and practices applied by certSIGN in providing the validation services for qualified signatures/seals applied to PDF documents.
This document is identified by: QSVS-PPS-EN and its version: v1.7 – 31 Mar.2026
certSIGN PPMB is responsible for the management of certSIGN Validation Service Practice Statement. This document is approved by the Policies and Procedures Management Body and is publicly available at certSIGN website https://www.certsign.ro/en/repository.
certSIGN will notify the Supervisory body about any significant changes in the provision of qualified trust services without undue delay but no later than 3 working days.
certSIGN will notify the Supervisory body about the planned termination of the qualified trust service no less than 3 months prior to the the termination of qualified trust service.
Subscribers and Relying parties will only take into account the effective version of certSIGN QSVS-PPS as of the time of using the services provided by certSIGN.
The latest and previous version of this practice statement will always be present at: https://www.certsign.ro/en/document/policies-and-practices-for-qualified-validation-service/

The **Terms of Use of Paperless Validation Service** document contains the terms and conditions established between the TSP and the final beneficiary of the trust service. The document identification is: Paperless QVSA and its version is in the document footer.
The latest version of the Terms and Conditions applicable to the Validation Service will always be present at: https://www.certsign.ro/en/document/qualified-validation-service-terms-of-use/
Older versions of this practice statement or Terms and Conditions are stored in archives and links to them will be provided on request.
The Global Information Security Policy of certSIGN is an internal document, available only to certSIGN members. The Information Security Policy applies to all the business lines of the company and covers the information, information systems, networks, physical environment and relevant people who support the services provided.
certSIGN Risk Management is a confidential document, available only to a certSIGN distribution group, that includes the analysis of the main threats & vulnerabilities, a risk assesment and the proposed solution for each considered risk.
certSIGN has implemented an Information Security Management System (ISMS) according to ISO/IEC-27001:2013 standard. certSIGN has achieved certification of ISMS according to ISO/IEC-27001:2013 standard.
certSIGN has implemented all necessary controls required by eIDAS and GDPR regulations and corresponding standards (i.e. ETSI EN 319 401) into ISMS. certSIGN Chief Executive Officer approves policies and practices related to information security.

2 Trust Service management and operation

certSIGN has implemented an Information Security Management System according to ISO/IEC 27001:2013 standard and has achieved ISO/IEC 27001:2013 certification by an accredited international certification body. Qualified Signature and Seal Validation Services are within the scope of this certification. The paragraphs below summarize management and operations of trust service, including security controls applied.

2.1 Internal organization

2.1.1 Organization reliability

certSIGN complies with all legal obligations applicable to the provisioning of its Trust Services. It conducts its operations in line with the adopted policies and practices.
certSIGN ensures that all requirements defined in ISO27001:2013 Statement of Applicability and this Practice Statement are implemented and remain applicable to the Trust Services provided.
certSIGN offers its Trust Services under non-discriminatory practices.
certSIGN has the necessary financial stability and resources for operation in accordance with this document. certSIGN maintains insurance of its civil liability in accordance with the applicable legislation, to cover obligations arising from its operations and in line with Article 13 of eIDAS regulation. certSIGN may provide more information about specific organization reliability measures upon special legitimate request from concerning party.
certSIGN fulfills general security requirements set out in article 19 of the eIDAS Regulation as further developed in ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
In relation to the validation Trust Services, certSIGN provides validation of (Qualified) Electronic Signatures and Seals in accordance with article 32 of the eIDAS Regulation and relevant sections of ETSI TS 119 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.
The Signature Service is provided in accordance with the applicable sections of the eIDAS Regulation, namely Recitals (52, 55) and Annex II.3.
The provision of Trust Services is subject to an external audit performed at least every 24 months by a Conformity Assessment Body and the qualified status is supervised by the Supervisory Body.
Records concerning the operation of the Trust Services are made available to affected parties upon legitimate request for the purposes of providing evidence of the correct operation of the Trust Services for the purposes of legal proceedings.
Subscribers are obliged to maintain confidentiality of passwords and applicable credentials to use the Validation Services and promptly communicate certSIGN any circumstance raising suspicion or risk of them being compromised.
certSIGN has appropriate insurance arrangements to cover certSIGN provision of Trust Services to ensure compensation for damages caused by an intentional or negligent violation of certSIGN obligations under the eIDAS Regulation.
certSIGN is not liable for:

- Any damage arising from a signatory or a Subscriber failing to maintain the secrecy of the OTP devices, passwords and applicable credentials to use the Signature Service or the Trust Services
- The non-performance of its obligations if such non-performance is due to faults or security

problems of any public authority
• Non-fulfillment of its obligations if such non-fulfillment is caused by a Force Majeure event.
Disputes related to Trust Services provided by certSIGN shall be settled initially through a conciliation procedure, during which both Parties shall in good faith negotiate solutions in respect of any disputes arising. certSIGN's TSP Board shall be responsible for handling such conciliation procedure. If the specific complaint is not settled within thirty (30) days of the commencement of the conciliatory process, the Parties may refer the dispute to the appropriate courts of Bucharest, Romania.
All confidential and proprietary information disclosed to certSIGN in the use of Trust Services shall be Confidential Information.
Confidential Information does not include information that:
• enters the public domain through no fault of certSIGN;
• is communicated by a third party to certSIGN free of any obligation of confidence;
• has been independently developed by certSIGN without reference to any Confidential Information of the disclosing party;
• was in certSIGN's lawful possession prior to disclosure and had not been obtained either directly or indirectly from the disclosing party, or
• is required to be disclosed by law, provided certSIGN has promptly notified the disclosing party in writing of such requirement and allowed the disclosing party a reasonable time to oppose such requirement.
Any external organization supporting the TSP services will be contractually constrained to follow the applicable policies and practices and to follow certSIGN approved procedures.
All the deployed versions of the QSVS modules are previously tested according to the approved Test Plan, in the testing environment, different use-cases, positive and negative.

2.1.2 Segregation of duties

Strict segregation of duties between development and operation of the platform is ensured organizationally and is being implemented technically. Security administration and operation roles are organizationally segregated and are strictly restricted to authorized personnel.
Implemented and certified Information Security Management System according to ISO/IEC 27001:2013 ensures that segregation of duties is verified and maintained. More specifically: Information security manager (ISM) and internal auditor roles are separated.
Also, the Policies and Procedures Management Body is established to deal with major issues, including issues in information security.

2.2 Human resources

certSIGN as a trusted service provider makes or ensures that the relevant checks are performed by specialized personnel.
Basic obligations with regards to security are set out in each person's working agreement: this includes confidentiality and non-compete clauses in contract.
Each prospective employee is assessed for the necessary proofs of qualification of professional training necessary to carry out the function concerned in a proficient and qualitative manner. If sufficient experience has been acquired in the actual work environment and can represent the equivalent of a professional training course (or courses), the relevant requirements are clearly mapped out in the vacancy and will be checked by reference to the proofs of experience submitted by the prospective employee.
Prior to employment:

- **Screening** - HR Management Policy is a part of ISMS. If defines recruitment, on-boarding and employment termination processes. Pre-employment checks and vetting, including checks on criminal convictions as required for Qualified Trust Service providers, employment history and references are part of certSIGN recruitment process.
- **Terms and conditions of employment** - Every employee signs a standardised form of an employment contract and confidentiality agreement before employment and actual work-related activities. In addition, an employee is getting familiarised with the list of business secrets which is approved by organisation's management body and all the information and data that fit into the defined categories need to be kept as a business secret and protected.

During employment:

- **Management responsibilities** - Management governs and supports ISMS activities and employees are one of the essential parts of ISMS. Governing process and management responsibilities are described in Information security policy and management practice document
- **Information security awareness, education and training** - Training and internal awareness activities are essential for personnel to understand the importance of information security management and their own contribution to ISMS, accept policies and plans, and understand the consequences of breaching the information security rules. As a result, training and awareness plan is prepared and coordinated by ISM and include regular updates (yearly) on new threats and current security practices. Its execution results in associated tangible records. All employees in Trusted roles fulfil the requirement of 'expert knowledge, experience and qualifications' through formal training and credentials, or actual experience, or a combination of the two.
- **Disciplinary process** - According to HR Management Policy, disciplinary actions are part of:
  - Labour Code of Romania;
  - Employment contract;
  - Special NDA clauses signed by an employee.
- **Termination or change of employment responsibilities** - According to the NDAs with employees, confidentiality statements remain valid after the termination of employment. The review of access rights should be performed as per Access Control Policy when changes in employment responsibilities occur.

2.3 Asset management

2.3.1 General practices

certSIGN maintains up-to-date lists of assets, inclunding information assets. Risk Management is based on the identification of assets. General requirements include:
Inventory of assets – certSIGN maintains up-to-date lists of all assets (both virtual and physical) and their owners. Organisation's risk assessment is aligned with the identification of assets and threats are identified as related to assets using elaborate mapping
Ownership of assets - maintains up-to-date lists of all assets (both virtual and physical) and their owners.
Acceptable use of assets - Acceptable Use Policy defines clear rules for the use of

information systems and other information assets at certSIGN. It also defines responsibilities, prohibited activities, taking assets off-site, returns of assets, backups, internet use within assets, mobile computing, teleworking.
Return of assets – certSIGN ensures that all the equipment, software and information in electronic and paper form is returned, where applicable.

2.3.2 Media handling

Media containing sensitive information is handled securely and in accordance with certSIGN Information Classification Policy and certSIGN Operating Procedures. Specifically:
Management of removable media - Information Classification Policy defines how to handle information in printed, electronic, electronic within information systems, and email formats, including removable media (and storage). It includes access, usage of passwords and encryption.
Disposal of media - Operating Procedures provides controls for disposal and destruction of equipment and media. In general, all equipment containing storage media (e.g. computers, mobile phones, etc.) must be wiped-out before it is reused or media destroyed before it is disposed of.
Physical media transfer - Information Classification Policy defines technical security controls for securing information in media, including for transfer, depends on the classification level. Operating Procedures provides requirement to wipe-out any kind of media before it is reused.

2.4 Access control

certSIGN operates a segmented network (users, development and production) where firewalls are in place.
Access to privileged operations are restricted by means of access controls, where a series of groups and profiles have been defined and assigned as per job responsibilities: these are designed to enforce segregation of duties and least privilege principle.
Access rights are allocated after management authorization.

Business requirements of access control:
Access control policy - The basic principle is that access to all systems, networks, services and information is forbidden ("denied by default"), unless expressly permitted ("need to know") to individual users or groups of users. Access control policy provides a comprehensive framework for (electronic) access provision, requirements for corporate account security settings, privilege management, and regular review of access rights. According to the policy, associate traceable access control records must be ensured and kept.
Access to networks and network services – The basic principle is that access to all systems, networks, services and information is forbidden ("denied by default"), unless expressly permitted ("need to know") to individual users or groups of users. Remote access is supported in an encrypted manner only (Operating Procedures) and is a subject to Acceptable Use Policy at certSIGN.

User access management:
User registration and deregistration – certSIGN Access Control Policy provides a framework for registering a user in the corporate directory, internal network and

information systems. Access control policy also provides user de-registration process, including requirements for accounts removal.
User access provisioning - The basic principle is that access to all systems, networks, services and information is forbidden ("denied by default"), unless expressly permitted ("need to know") to individual users or groups of users. Remote access is supported in an encrypted manner only (Operating Procedures) and is a subject to Acceptable Use Policy.
Management of privileged access rights - privileges for each system (asset) may be granted only by their respective owners or PPMB.
Management of secret authentication information of users - Acceptable Use Policy provides comprehensive requirements for users to manage and use secret authentication information.
Review of user access rights - Regular review of access rights is defined in Access Control Policy.
Removal or adjustment of access rights - Access rights are being removed or adjusted by following the Access Control Policy. Despite a timely change of access rights upon business requests, the responsible manager guarantees and ensures that access rights for every system/sub-system/component are reviewed at least once per year.

User responsibilities:
Use of secret authentication information - Acceptable Use Policy provides comprehensive requirements for users to manage and use secret authentication information. It enforces best industry practices, like using encrypted password management tools.

System and application access control:
Information access restriction - The Information Classification Policy defines information access restriction and provision procedures. In addition, the Access Control Policy defines the basic principle that access to all systems, networks, services and information is forbidden ("denied by default"), unless expressly permitted ("need to know") to individual users or groups of users.
Secure log-on procedures - (Electronic) access provision rules in Access Control Policy requires that access to the internal, external or third party service/application should be provided by using federated corporate account authentication service.
Password management system - Detailed requirements for corporate account security settings are listed in the Access Control Policy, which reflects industry best practices.
Use of privileged utility programs - There is a limitation in Acceptable Use Policy that users must not take part in activities which may be used to bypass information system security controls.
Access control to software source code - The program source code is intellectual property and is accessible on a basis need-to-know only. Information Classification Policy defines authorised persons and access restrictions to business secrets (program source code is a part of business secrets). Physically source code is stored in the Source Code Versioning system, where ISM provides key-based access to required sources.

2.5 Cryptographic controls

Data at rest and transit are encrypted using industry standards.
Cryptographic controls:

Policy on the use of cryptographic controls - Policy on the Use of Cryptographic Controls defines rules (regulation) for the use of cryptographic controls, as well as the rules for the use of cryptographic keys, in order to protect the confidentiality, integrity, authenticity and non-repudiation of information.
Key management - Policy on the Use of Cryptographic Controls defines the management of keys, including their distribution practices.
certSIGN CAs are using hardware key protection which is complying at least with FIPS 140-2 level 3 or Common Criteria EAL 4 standards. CA key pair generation shall be carried out within a secure cryptographic device which is a trustworthy system complying at least with FIPS 140-2 level 3 or Common Criteria EAL 4 standards.

In certSIGN, as a QSVSP, the service implementation complies with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA for use of suitable cryptographic techniques when providing qualified validation services for QES.

certSIGN's private signing key are exported and imported into a different secure cryptographic device, only with PPMB approval, like to the DR site, where this export and import are implemented securely and in accordance with the certification of the HSM devices.

2.6 Physical and environmental security

Physical access to offices & data center facilities is appropriately restricted to authorized personnel. Safeguard measures are in place to protect critical assets and ensure continuity. Physical access is controlled and monitored by an integrated alarm system. Fire prevention system, intrusion detection system and emergency power system are in place.
CERTSIGN work schedule is from Monday to Friday between 9.00 and 18.00. Outside this time interval, including public holidays, access to CERTSIGN premises is allowed only to persons authorized by the Management of CERTSIGN.
Visitors are permanently escorted by the authorized personnel.
CERTSIGN premises are divided into:

- Office areas,
- IT areas,
- CA operators area
- RA operators and administrators area,
- Developing and testing area.

IT areas are equipped with monitored security system built on the basis of motion, intrusion and fire. Access to this area is granted only to authorized personnel. Monitoring of access rights is carried out based on electronic cards and appropriate readers, mounted next to the entry area. Every entry to and exit from the area is automatically recorded in the event log.

Access to the operators' area is allowed only based on an electronic card and its appropriate reader. Since all sensitive information is protected by the use of locked cabinets, while access to operator's or administrator's terminal requires prior authorization, the implemented physical security is considered adequate. Keys to the area are accessible only to authorized personnel. The area may be occupied solely by CERTSIGN personnel and authorized individuals, the latter being granted access only if accompanied.

Unattended individuals are not allowed in this area. Programmers and developers do not have access to sensible information. If such access is necessary, the presence of the

security administrator is required. Projects being implemented and their software are tested on the development environment of CERTSIGN.

2.7 Operation security

In terms of Change Control, for every change or project to the certSIGN platforms, functional and technical analysis is conducted and includes an identification of appropriate security measures required. Changes are controlled by means a formal incident and change management process.
Anti-malware protection is enabled, and removable media use is limited, and does not support business critical activities.
Windows servers and SQL databases are patched periodically, leveraging default platform functionalities. A patch management process is formally defined. certSIGN uses application environment that is maintained with up-to-date security fixes to ensure that the systems on which the application is developed apply appropriate security measures and adapt to specific application environments.
CERTSIGN uses trustworthy systems and products that are protected against modification and ensures the technical security and reliability of the processes supported by them.

certSIGN uses well-tested and reviewed implementations of standardized protocols and libraries within all the implementations and configurations of the applications used.

2.7.1 Specific computer security technical requirements

Security mechanisms protecting computer systems are executed at the level of operating systems, applications and physical protections.

Computers are configured with the following security mechanisms:

- Mandatory authenticated registration at operating system and applications level,
- Discretionary access control,
- Possibility of conducting security audit,
- The computer is accessible only to authorized personnel, performing trusted roles in CERTSIGN,
- Enforcement of duty segregation, arising from the role performed in the system,
- Identification and authentication of roles and personnel performing these roles,
- Prevention of an object re-use by another process after the object was released by an authorized process,
- Cryptographic protection of information exchange and protection of databases,
- Archival of operation history on the computer and of data required by audits,
- A secure path allowing reliable identification and authentication of roles and of personnel performing these roles,
- Key restoration methods (only for hardware security modules),
- Monitoring and alerting in case of unauthorized access.

The integrity of CERTSIGN systems and information is protected against viruses, malicious and unauthorized software.

Media used within CERTSIGN systems are securely handled to protect media from damage, theft, unauthorized access and obsolescence.

Media management procedures are implemented to protect against obsolescence and deterioration of media for the period of time for which records must be kept.

Sensitive data is protected against disclosure through re-used stored objects (e.g. deleted files) being inaccessible to unauthorized users. For that purpose, special software shall be used with secure deletion algorithms for storage media, HSMs shall be zeroized, secure cryptographic devices (tokens/cards) shall be formatted before reuse/, or physically destroyed at the end of their life cycle.

2.7.2 System development controls

An analysis of security requirements is carried out in design and requirements specification stage of system development projects undertaken by CERTSIGN or on behalf of CERTSIGN in order to ensure that security is built into IT systems.

Every application, prior to be used for production within CERTSIGN, is installed so as to allow control of the current version and to prevent unauthorized installation of programs or forgery of existing ones.

Similar rules apply to hardware components replacement, as follows:

- Hardware is supplied in a manner that allows traceability and monitoring of the route of components to the place of their installation,
- Spare hardware delivery is carried out in a manner similar to delivery of original hardware; the replacement is carried out by trusted and trained personnel.

2.7.3 Security management controls

The purpose of security management control is to supervise CERTSIGN systems' functionality providing assurance that the system operates correctly and in accordance with the accepted and implemented configurations.

Controls applied to CERTSIGN system allow continuous verification of application integrity, of their version as well as authentication and verification of hardware origin.

2.7.4 Life cycle security controls

Change control policies and procedures are applied for releases, modifications and emergency software fixes of any operational software and changes in configurations applying CERTSIGN's security policy.

Current configuration of CERTSIGN systems, any change or new release, modification and emergency software fixes of any operational software are documented.

Configurations of Production Systems, Management Systems, Security Support Systems, and Front-End / Internal-Support Systems are periodically reviewed to determine whether any changes violated the CA's security policies

CERTSIGN implements internal security procedures for ensuring that:

- Security patches are applied within a reasonable time after they come available;
- Security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them;

The reasons for not applying any security patches are documented.

CERTSIGN implements an internal capacity management procedure which ensures that the capacity of ICT infrastructure for production services is monitored and that estimates of

capacity requirements are made to ensure that adequate processing power and storage are available.

2.8 Network security

CERTSIGN protects its network and systems from attack. For that purpose and based on risk assessments and best practices we implement an integrated set of security controls:

a) Systems are segmented into networks or zones based on the functional, logical, and physical (including location) relationship between trustworthy systems and services. CERTSIGN applies the same security controls to all systems co-located in the same zone.
b) Access and communications between zones are restricted to those necessary for the operation of production services. Unnecessary connections and services are explicitly forbidden or deactivated. The established set of rules is reviewed on a regular basis.
c) All systems that are critical to the production services operation are kept in one or more secured zone(s)
d) Dedicated network for administration of IT systems and operational network are separated. Systems used for the administration of security policy implementation are not used for other purposes. The production systems for the production services are separated from systems used in development and testing (e.g. development, test and staging systems).
e) Communication between distinct trustworthy systems are established only through trusted channels that are logically distinct from other communication channels and provide secured identification of its end points and protection of channel data from modification or disclosure.
f) If a high level of availability of external access to a specific certification service is required, the external network connection is redundant in order to ensure availability of the services in case of a single failure.
g) Regular vulnerability scan on public and private IP addresses identified by CERTSIGN is performed and evidence is recorded that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.
h) CERTSIGN production services undergo a penetration test on the related systems upon set up and after infrastructure or application upgrades or modifications that CERTSIGN considers to be significant. Evidence is recorded that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

Servers and trusted workstations of CERTSIGN system are connected by a local network (LAN), divided into sub-networks provided with controlled access. Access from the Internet to any segment is protected by means of intelligent firewall.

Security controls are developed based on firewall and traffic filtering on the routers and Proxy services that protect CERTSIGN's internal network domains from unauthorized access including access by Subjects/Subscribers and third parties. Firewalls are configured to prevent all protocols and accesses not required for the operation of CERTSIGN CA.

Means of protection of the network security accept only messages submitted with the use of http, https, NTP, POP3 and SMTP protocols. Events (logs) are recorded in system journals and allow supervision of the use of services provided by CERTSIGN.

CERTSIGN maintains and protects all critical systems in at least one secure zone and has in place a security procedure that protects systems and communications between systems inside secure zones and high security zones.

CERTSIGN configures all critical systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the effective operations.

CERTSIGN grants access to secure zones and high security zones only to trusted roles.

2.9 Incident management

Logging leverages default platform functionalities, both at host and account level. Log monitoring is performed reactively, to ensure analysis of anomalous behavior. A formal incident management process is defined, and dedicated information security incident management process.

2.10 Collection of evidence

certSIGN maintains records concerning the operation of the Trust Services for the purposes of providing evidence of the correct operation of the Trust Services. These records will only be disclosed to law enforcement authorities under court order and to persons with right to access to them upon legitimate request. These records are maintained under confidentiality in facilities to ensure availability throughout the period they are maintained.
In order to manage efficiently the systems and applications used by CERTSIGN in its activity as a trusted services provider but also in order to audit the employees and customers actions, all the information about important, specific events generated by the systems and applications are recorded. That information, collectively known as logs is kept in such way that it can be accessed by the Relying Parties, auditors and state authorities at any time they need it, in order to provide evidence of the correct operation of the services for the purpose of legal proceedings or to detect attempts to compromise CERTSIGN's security. The recorded events are backed-up and kept in a secondary location.

Whenever possible the logs are created automatically. If this is not possible logs on paper will be used. Each record in a log created either automatically or by hand is preserved or disclosed during an audit, if required. The time accuracy of logs is ensured by a time server that is synchronized with at least two different time sources that can be GPS satellites or UTC (NIMB).

2.10.1 Types of events recorded

Every critical activity from CERTSIGN's security point of view is recorded in event logs and archived. The archives are stored on storage media that cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held. CERTSIGN event logs contain recordings of all activities generated by the software components within the system. These recordings are divided into three distinct categories:

- **System logs** – contain information about customer's requests and server's responses (or vice versa) at the level of the network protocol (for example http, https); the recorded data is: IP address of the station or server, performed operations (for example: searching, editing, writing etc.) and their results (for example the successful entry of a record in the database),
- **Errors** – contain information about errors at the network protocols level and at the applications' modules level;

- **Audit logs**– contain information specific for the production services, for example: validation request, document check request, signature/seal acceptance, etc.

The above logs are common to every component installed on a server or on a workstation and have a predefined capacity. When this capacity is exceeded a log version is automatically created. The previous log is archived and deleted from the disk.

Every automatic or manual recording contains the following information:

- Event type,
- Event identifier,
- Event description,
- Date and time of the event occurrence,
- Identifier of the person in charge with the event.

All events relating to the life-cycle of certificates used with signatures/seals are recorded.

CERTSIGN maintains internal logs of all security events and all relevant operational events in the whole infrastructure whatever the component service, including, but not limited to:

- Changes to the security policy
- Start and stop of systems;
- Outages;
- System crashes and hardware failures
- Firewall and router activities
- PKI system access attempts
- Physical access of personnel and other persons to sensitive parts of any secure site or area;
- Back-up and restore;
- Report of disaster recovery tests;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.

Access to logs is exclusively allowed for the security officer, special appointed personnel, and auditors.

The privacy of subscriber information is maintained.

2.10.2 Frequency of processing log

Logs are processed continuously and/or following any alarm or anomalous event. Logs are regularly archived and backed-up.

2.10.3 Retention period for audit log

Events' records are stored in files on the system disk until they reach the maximum allowed capacity. This whole time, they are available on-line, upon every authorized person's or process request. After exceeding the allowed capacity, journals are kept as archives and can be accessed exclusively off-line, from a certain workstation.

The archived journals of logs are kept 3 years.

2.10.4 Protection of audit log

The log files are properly protected by an access control mechanism. Appropriate protection against modification and deletion of the audit logs is implemented such that no one may modify or delete audit records except after transfer to long term media for archiving purposes.

Only the security officer, special appointed personnel, or an auditor can review an event journal. The access to the events journal is configured in such way that:

- Only the above entities have the right to read the journal's records,
- The central log platform automatically archives or deletes files (after their archiving) that contain recorded events,
- It is possible to identify any integrity violation; this thing ensures that the records do not contain gaps or forgeries,
- No entity has the right to modify the content of a log.

Moreover, the log protection controls are in such a way implemented that, even after log archiving it is impossible to delete records or the log as a whole before the expiration of the log global retention time.

2.10.5 Audit log backup procedures

CERTSIGN security policies require that the event journal should have a periodical backup. These backups are stored in auxiliary locations of CERTSIGN. Log files and audit trails are backed up according to internal procedures.

2.10.6 Audit collection system (internal vs. external)

All the logs generated by servers, network devices, security equipment, applications are continuously sent to a central platform, whose purpose is to:

- Collect
- Store
- Analyse
- Correlate
- Archive
- Long term Back-up

2.11 Business continuity management

A business continuity and disaster recovery plan are in place.
CERTSIGN has established in a Business Continuity and Disaster Recovery Plan all the necessary measures to ensure full recovery of its services in case of a disaster, or a disruption of any important IT&C component or service longer that the established Maximum Tolerable Downtime. Any such measures are compliant with the ISO/IEC 27001 and 27002 standards. For each component or service operations will be restored within the Maximum Tolerable Downtime established in the continuity plan.

All data from the systems required to resume production operations are backed up and stored in a remote and safe place, suitable to allow trusted services to timely go back to operations in case of incident/disasters.

Back-up copies of essential information and software are realized regularly. Adequate back-up facilities are provided to ensure that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements are regularly tested to ensure that they meet the requirements of business continuity plans.

Backup and restore functions are performed by the relevant trusted roles.

Following a disaster, where practical, steps will be taken to avoid repetition of a bad steps.

2.12 TSP termination and termination plans

CERTSIGN has an up-to-date termination plan to minimize disruptions to Subscribers and Relying Parties which might arise from a decision to cease an activity/service. The plan includes obligations to notify in advance all Subscribers of the TSP service subjected to termination (if such exists) and transition of responsibilities, in compliance with the regulations in force to another Trusted Services Provider.

Requirements associated to duty transition

Before a TSP ceases its activity, it will:

- Inform (at least 30 days in advance) about the decision to terminate its services: all Subscribers with which CERTSIGN has agreements or other form of established relations, among which relying parties, other trust service providers and relevant authorities such as supervisory bodies. In addition, this information will be made available to other relying parties;
- Transfer its obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the production services for a reasonable period, unless it can be demonstrated that CERTSIGN does not hold any such information. The information refers to validation information, and event log archives for their respective period of time as indicated to the Subscriber and involved relying parties;
- Where possible, make arrangements to transfer provision of validation services for the existing customers to another trusted service provider.

In case CERTSIGN will terminate its activities without a partially or full transfer of its activities, it will initiate the termination procedure for the contracts signed with the implied partners and/or supliers.

CERTSIGN has an arrangement to cover the costs to fulfil these minimum requirements in case it becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

2.13 Compliance

The operational procedures define the process of signature validation for the interested parties, as well as legal, regulatory, contractual and other requirements and responsibilities for their fulfilment.

Identification of applicable legislation and contractual requirements - An operational procedure includes the process of signature validation for the interested parties, as well as legal, regulatory, contractual and other requirements related to information security, and responsibilities for their fulfilment. Activities result in the maintained and actual List of legal, regulatory, contractual and other requirements.

Intellectual property rights - Intellectual property rights are part of Business secrets defined by the PPMB. It is regulated according to the EU and local legislation. Protection of intellectual property rights results in NDAs, contractual obligations and responsibilities and terms of certSIGN services.

Protection of records - An operational procedure ensures control over creation, approval, distribution, usage and updates of documents and records used in the ISMS. In general, employees of the organization may access stored records by following the principle "need to know" only.

Privacy and protection of personally identifiable information – certSIGN TSP activities are subject to EU GDPR regulation, requirements of which are properly incorporated into the organisation, including ISMS documentation. From specific service/processes/asset owners perspective, service/processes/asset owners are responsible for each individual requirement identification (including contractual) and compliance within the asset.
Regulation of cryptographic controls – certSIGN Policies define rules (regulation) for the use of cryptographic controls, as well as the rules for the use of cryptographic keys, in order to protect the confidentiality, integrity, authenticity and nonrepudiation of information.
Miscellaneous provisions - certSIGN provides unlimited access to services for people with disabilities in accordance with current legislation and standards.

2.14 Supply chain

certSIGN documented and implemented processes and procedures to manage the information security risks associated with the use of supplier's products or services. They are detailed in the internal certSIGN policy for the management of the third -party providers (" *Politica de Management al Serviciilor Furnizate de Terti*").
The process and the procedures implemented are managing the information security risks associated with the information and communication technologies products and services supply chain, as requested in ETSI EN 319 401 #7.14.
When certSIGN makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third party arrangements, it maintains overall responsibility for conformance with the supply chain policy, its information security policy and the requirements defined in the trust service policy.
certSIGN review the supply chain policy and monitor, review, evaluate and manage changes in the cybersecurity practices of direct suppliers or service providers at planned intervals or after an incident related to the provision of services from direct suppliers or service providers.

3 Signature Validation Service Design

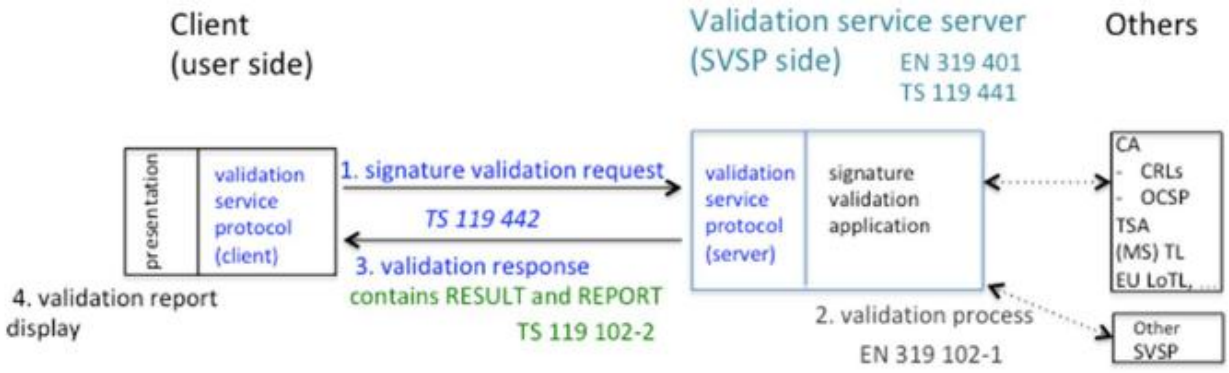
The service may only be used by certSIGN contractual customers. The Service can only be accessed using defined interfaces published by certSIGN.
The Subscriber of the Service is obligated to protect the Service interface from unauthorized use and provide appropriate security when using the Services. This applies to any interface used to access this Service.
The interface means, in particular, the web application for using the Service or any application or integration interface supplied exclusively by certSIGN or an integrator specified by certSIGN.

3.1 Signature Validation process

When specific requirements and rules are set in the present specification, they shall prevail over the corresponding requirements from ETSI TS 119 102 or ETSI TS 119 441. In case of discrepancies between the present specifications and specifications from ETSI TS 119 102 or ETSI TS 119 441, the present specifications shall prevail.

3.1.1 Signature Validation process flow

The process is conform to ETSI TS 119 441 V1.2.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.



Depending on the chosen validation mode, the Client sends a validation request to the certSIGN SVSP that contains the document(s) to be validated together with signatures and complementary transactional parameters.
The certSIGN service parses the request and

- when successful
  - performs the validation on the input
  - creates a validation report
  - seals the created report and
  - returns a response comprising the sealed report
- otherwise
  - returns an error message

In this respect, the certSIGN validation service operates independently of APP's context.

For the purpose of matching a digest value with signed data, it is important:

- To apply the digest algorithm which had been specified during signature creation,

- That the applied digest algorithm is considered secure at the time of signing and has not become weak until the time of validation or has been protected by complementary preservation means,
- That the implementation for (re-)calculating the applied digest algorithm is correct and trustworthy and
- That any explicit or implicit transformation of input bytes for calculating the corresponding digest value is correct with respect to the media type of the given input document. For instance, in the case of a PDF document, the byte ranges indicated in the signature dictionary directly specify the input bytes for digest calculation, while in the case of a generic document explicitly or implicitly defined content transformations might be necessary in order to obtain the input bytes for digest calculation.

Following ETSI EN 319 102-1 V1.3.1 (2021-11) *„Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"*, the validation process provides, for each signature, one of the following three status indications:

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

3.1.2 Signature Validation and Conformance Checking

The conceptual model of the signature validation and conformance checking:

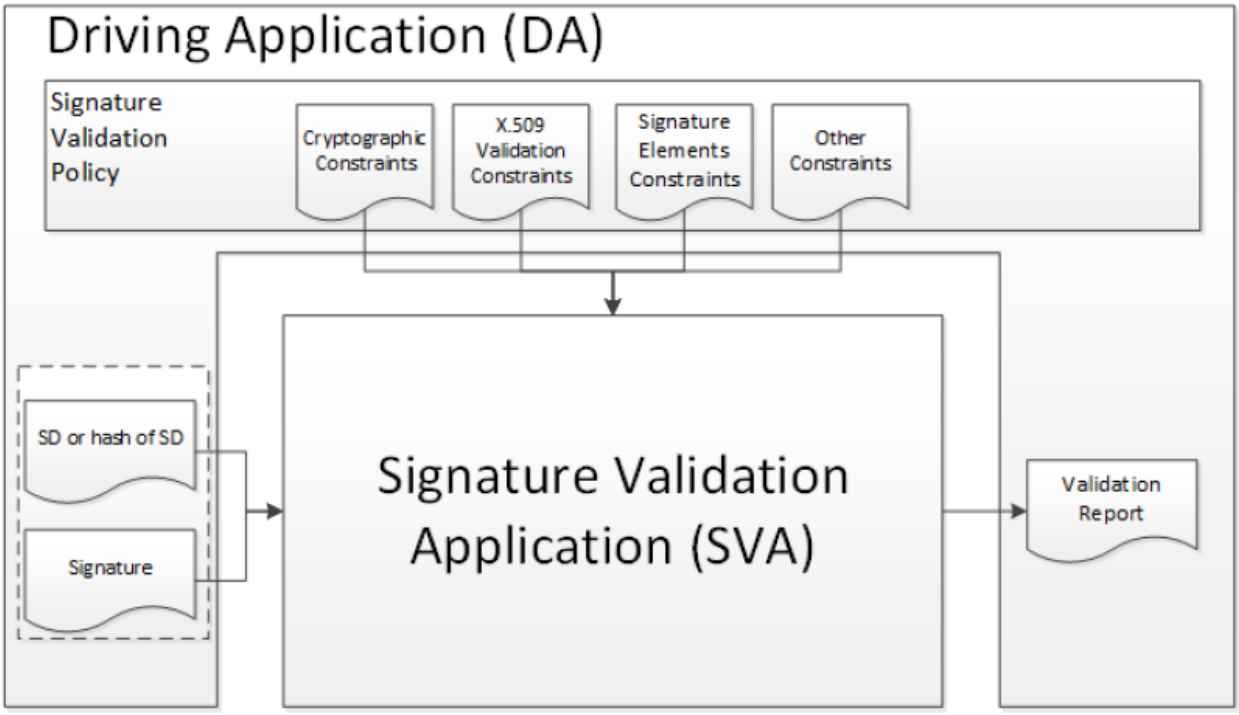


Figure 2 Signature Validation Model with Conformance Checking included in SVA

While signature validation is the process of verifying and confirming that a signature is technically valid, conformance checking determines whether a signature complies with the requirements of a specification or regulation. Thus, signature validation and conformance checking of signatures are independent processes:

- A signature can be valid but not conformant to a certain signature level required.
- A signature can be conformant to a certain signature level but validation may return an INDETERMINATE or TOTAL-FAILED status indication.

While conformance checking is in principle orthogonal to signature validation (a signature may be valid, but not conformant), conformance checking can be required by a signature validation policy for specific business contexts.

For each of the validation checks, the validation process provides 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 subindications.

The validation process is driven by the validation policy and allows long term signature validation. The signature check is done following the basic building blocks of the validation algorithm.
On the simplified diagram below, showing the process of the basic signature validation, you can follow the relationships between each building block which represents a logic set of checks used in the validation process.

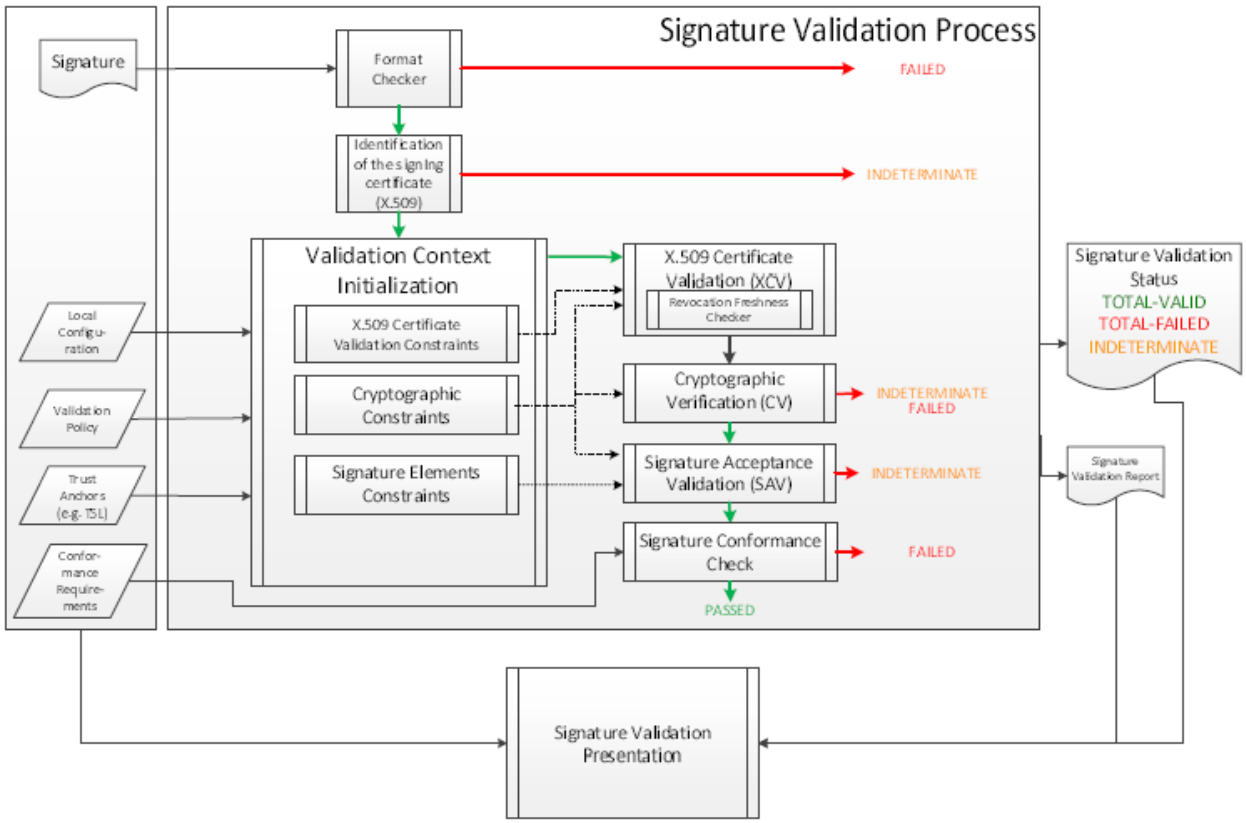


Figure 3 Conformance Checking as part of Signature Validation

certSIGN validates the signature against a signature validation policy, consisting of a set of validation constraints, and outputs a status indication and validation report providing the details of the technical validation of each of the applicable constraints (e.g. expired certificates or timestamps, revoked certificates, usage period of cryptographic algorithms exceeded).

certSIGN QSVS is conforming to ETSI TS 119 172-4 Validation constraints and validation procedures (chapter 4.2), supports the Requirements on signature validation and applicability rules checking practices (chapter 4.3), and implemented the Technical applicability (rules) checking process (chapter 4.4). The report is implemented in accordance to Requirements on applicability rules checking report (chapter 4.5).

3.1.3 EU Trusted Lists of Certification Service Providers

In order to allow access to the trusted lists of all Member States in an easy manner, the European Commission has published a central list with links to national "trusted lists" (LOTL).
The LOTL is published by the EU at the following URL :
https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.
This XML file contains the list of the trusted list. This file must be signed by an allowed certificate. To know who has the permission to sign / publish the LOTL, we need to refer to the Official Journal Of the Union (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2016.233.01.0001.01.ENG).

If the LOTL signature is valid, the content can also be trusted. It contains some information for each country: URLs of the XML / PDF files, the allowed certificates to sign, … When trusting the LOTL, we can process each TL. If they are valid, we can trust the service providers and its certificates.
This LOTL is then used to perform the certificate validations that are needed in the context of a signature validation. The SVS builds the certificate path until a known trust anchor, validates each found certificate (using OCSP when possible, otherwise CRL) and determines its European "qualification".
To determine the certificate qualification, the SVA follows the standard Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists (ETSI TS 119 172-4). It analyses the certificate properties and applies possible overrules from the related trusted list.
The SVA will always computes the status of the certificate for two different times: certificate issuance and signing / validation time. This is a necessity since the certificate qualification can evolve over time.

3.2 Signature Validation protocol requirements

The signature validation protocol is as follows:
1. the SVC sends the SD containing the digital signature(s) to be validated to the SVS
2. the SVS sends the signature validation response containing the SVR to the SVC

3.3 Interfaces

3.3.1 Communication channel

Communication between DA and SVS occurs via a secured TLS connection. This ensures confidentiality of the transmitted data and offer a way for both parties to authenticate each other.

3.3.2 SVSP - other TSP

Communication between the SVSP and other TSPs depend upon the interface that is defined and the requirements of the TSP that needs to be called.
The SVS setup TLS connections or other authentication means to communicate with external actors.

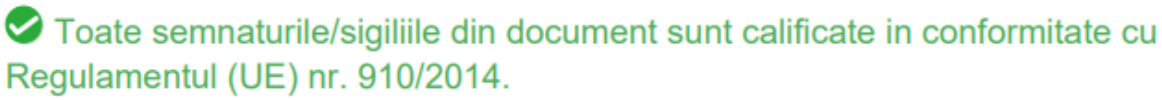
3.4 Signature Validation report

The machine readable report is conform to ETSI TS 119 102-2 V1.3.1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures Part 2: Signature Validation Report. certSIGN uses the schema required in ETSI: https://forge.etsi.org/rep/esi/x19_10202_validation_report/raw/v1.3.1/1910202xmlSchema.xsd.
The signature validation service report contains:

- The name of the document validated
- The Hash of the document and the algorithm used
- The date and time of the validation
- a status indicating the global result of the signature validation on the document;
- the list of digital signatures included in the document;
- For each digital signature:
    - The status of the signature validation and conformance checking

  - The name of the signer from the certificate
  - The issuer of the signature/seal certificate with the common name & organizationIdentifier
  - The date and UTC time of signing
  - The issuer of the time stamp certificate with the common name & organizationIdentifier
  - The status of the time stamp validation and conformance checking
- The identification of the QSVS and it's version;
- The qualified seal of certSIGN TSP with time stamp for non-repudiation

certSIGN conformance checking is against the EU Regulation Art.32 „Requirements for the validation of qualified electronic signatures". So only a PDF document with all signatures validated as TOTAL-PASSED and all signatures conformant to the EU Regulation will have a resolution at the document level marking that all signatures/seals are EU qualified:



The validation report is signed

4 Appendix 1 - Business Scoping Parameters

The description of the validation policies general business scoping parameters (BSP) is applicable to all business cases and is independent of the employed signature format.

4.1 BSPs Mainly Related to the Concerned Application/Business Process

BSP (a): WORKFLOW (SEQUENCING AND TIMING) OF SIGNATURES

The present validation policies address validation of the advanced electronic signatures and qualified electronic signatures comprising possible timestamps and proof-data extensions regarding a single instance or multiple instances of DTBS during a single transaction, while a single report is returned by the service after a successfully performed validation. A DTBS can consist of any binary data that shall specifically represent a PDF document. In case of multiple signatures embedded in the same PDF document, the signatures shall be serial.
The validation order is irrelevant.certSIGN validation service can be used by a Client/APP to implement business workflows comprising multiple transactions; in such a case, each single transaction within the Client/APP workflow will be performed according to the present policy depending on the chosen validation mode.

BSP (b): DATA TO BE VALIDATED

The Client/APP is responsible for the content and the correct formatting of the data to be validated with respect to applicable standards. In particular, it must ensure that the data to be validated does not contain malicious code or scripts that could alter the data to be validated or damage certSIGN services.
In particular, the format of an SD can be only PDF.
The certSIGN validation service guarantees the confidentiality of an SD according to applicable laws on privacy and Romanian laws regarding the financial sector. certSIGN particularly and immediately erases all copies of a received SD, if any, from its servers after having performed a requested transaction.

BSP (c): THE RELATIONSHIP BETWEEN SIGNED DATA AND SIGNATURE(S)

The relationship between signed data and signature(s) specifically depends on the signature format. certSIGN validation service supports the PAdES format which means that the signature is enveloped in the PDF document.
The supported signature profiles/levels are:
1. B-B (basic signature)
2. B-T (signature with time)
3. B-LT (signature with long-term validation material)
4. B-LTA (Signatures providing long-term availability and integrity of validation material)

BSP (d): TARGETED COMMUNITY

Unless otherwise specified within a derived Client/APP validation policy, the certSIGN validation service validates signatures based on the European trusted lists and complies with the eIDAS Regulation.

BSP (e): ALLOCATION OF RESPONSIBILITY FOR SIGNATURE VALIDATION AND AUGMENTATION

In addition to the clock of the service host, which is synchronized with a trustworthy accurate time source, the certSIGN validation service employs trusted and qualified timestamps according to the request profile (B-T, B-LT or B-LTA) as a proof of existence

regarding elements of the DTBS that are cryptographically covered by the given timestamps.
The certSIGN validation service validates existing signatures on the DTBS. Should the DTBS contain an invalid signature, that information is indicated in the result supplied by the service. certSIGN will NOT abort the validation process due to an invalid signature being contained in the DTBS.
A single validation report supplied by the certSIGN validation service may contain results regarding multiple signatures pertaining to an SD, while any interpretation of those results or an overall diagnostics of the outcome, in particular any semantic interrelationship of independently validated signatures, is completely left up to the business application. The certSIGN validation service does not perform any semantic interpretations; it solely provides diagnostics regarding individually validated signatures in accordance with the applicable standards.

4.2 BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process

BSP (f): LEGAL TYPE OF THE SIGNATURES

The certSIGN validation service supports validation for all legal types of qualified electronic signatures for legal persons or for physical persons that act on their own behalf or on behalf of a legal person:

- Qualified electronic signatures supported by an X.509 v3 qualified certificate;

The legal type of a signature is indicated in the validation report when it can be validated successfully.

BSP (g): COMMITMENT ASSUMED BY THE SIGNATORY

The certSIGN validation service can reveal the commitment type when associated with a given signature for being taken into account by the business application.
The validation service does not interpret a commitment type that is associated with a signature.

Commitment types

The following generic commitment types are defined in ETSI TS 119 172-1:

1) **Proof of origin**

- Description: It indicates that the signer recognizes to have created, approved and sent the signed data.
- Object identifier: id-cti-ets-proofOfOrigin OBJECT IDENTIFIER ::= { iso(1) member-body(2)us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 1}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfOrigin.

2) **Proof of receipt**

- Description: It indicates that signer recognizes to have received the content of the signed data.
- Object identifier: id-cti-ets-proofOfReceipt OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 2}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfReceipt.

3) **Proof of delivery**

- Description: It indicates that the TSP providing that indication has delivered a signed data in a local store accessible to the recipient of the signed data.
- Object identifier: id-cti-ets-proofOfDelivery OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 3}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfDelivery.

4) **Proof of sender**
- Description: It indicates that the entity providing that indication has sent the signed data (but not necessarily created it).
- Object identifier: id-cti-ets-proofOfDelivery OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 3}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfSender.

5) **Proof of approval**
- Description: It indicates that the signer has approved the content of the signed data.
- Object identifier: id-cti-ets-proofOfApproval OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 5}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfApproval.

6) **Proof of creation**
- Description: It indicates that the signer has created the signed data (but not necessarily approved, nor sent it).
- Object identifier: id-cti-ets-proofOfCreation OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) cti(6) 6}
- URI: The URI for this commitment is http://uri.etsi.org/01903/v1.2.2#ProofOfCreation.

BSP (h): LEVEL OF ASSURANCE ON TIMING EVIDENCES

To establish the time of the signature, the certSIGN validation service uses the following time evidence types:

- A claimed signing time;
- Trusted or qualified time stamps based on trust anchors that are verifiable according to the Member States trusted list.

Any such indication, except for a claimed signing time, may not only serve as a proof of existence used by the service to perform validation of signatures beyond the validity period of involved certificates, but it can also represent a trustworthy time indicator for the business application in order to make workflow decisions on its own discretion.
The certSIGN validation service can process only time stamps that comply with RFC 3161.
The certSIGN validation service does not interpret timing evidences beyond the fact of using them for performing signature validation.
The certSIGN validation service will include all the time evidences found in the processed signatures.

BSP (i): FORMALITIES OF SIGNING

The certSIGN validation service applies the validation procedures to the PDF document provided as input by the user.
The certSIGN validation service reveals in the final status report the associated signature attributes.

BSP (j): LONGEVITY AND RESILIENCE TO CHANGE

The expected longevity of an electronic signature depends on its profile.
B-B signature: the signature's longevity is that of the signing certificate at the time of signing, unless the signer certificate or any ancestor certificate in the issuer chain up to the trust anchor has been revoked after signing, which in that case would instantly render the signature unverifiable.
B-T signature: the signature's longevity is that of the signing certificate at the time of signing and is possibly extended beyond its lifetime when suitable online certificate status proofs are available. The time of signing is in this case confirmed by means of a signature

timestamp, with the signature timestamp being a pre-requisite for such an extended longevity beyond the lifetime of the signing certificate. Extended longevity can be supported in this case up to the longevity of the timestamping certificate at the time of signature timestamp creation. Contrarily to a B-B signature, revocation of the signing certificate or revocation of any ancestor thereof after creation of the signature timestamp has no impact on the longevity of a B-T signature. By contrast, extended longevity of a B-T signature can be impacted when a cryptographic algorithm, which was involved in the creation of the signature timestamp, has becomes weak over time.

B-LT signature: the signature's longevity is that of the above-cited B-T signature. It is augmented by proof elements added to the signed data object for partly enabling offline validation of the signature depending on the longevity and eligibility of added proof data. It is important to note that longevity of a signature is not extended beyond that of aforementioned B-T augmentation, solely due to the use of additional offline status proofs. However, B-LT augmentation can facilitate the overall validation process and serve as preparatory step for B-LTA augmentation.

B-LTA signature: the signature's longevity is that of the above-cited B-T or B-LT signature. It is augmented with complete proof elements regarding pre-existing elements of the signed data object that are needed for validation of the signer's signature, with the entire structure being covered by a document/archive timestamp. This enables extension of signature longevity up to the longevity of the timestamping certificate of that covering document/archive timestamp at the time of its creation. This maximum signature longevity extension also requires that all proofs added for the sake of augmentation are eligible and remain during the desired period assessable as valid at the time of document/archive timestamp creation, while such an assessment also relies on availability of suitable online status proofs. An extended longevity of a B-LTA signature can be impacted when a cryptographic algorithm, which was involved in the creation of the document/archive timestamp, has become weak over time.

A B-LTA signature can repeatedly be augmented by adding an enveloping B-LTA structure, whenever timely necessary due to the risk of expiration of any involved proof element or exceptionally, due to premature weakness of a cryptographic algorithm employed by any of the involved proof elements that have been added since the preceding B-LTA augmentation. It has to be kept in mind that creation of a new document/archive timestamp protects cryptographic algorithms of all covered structures from becoming weak provided that the algorithms used for creating that new timestamp remain resilient or are otherwise covered by another resilient timestamp prior to becoming weak.

A B-LTA signature can repeatedly be augmented as often as necessary for spanning the entire required period of longevity of the initial signer's signature. As an alternative to repeated B-LTA augmentation, a centralized electronic signature preservation service may be employed to ensure an equivalent period of longevity.

In any case, the cryptographic algorithms and parameters are verified with regard to applicable cryptographic standards in order to ensure that the electronic signature's resilience can be confirmed for a given signed artefact with respect to the closest proof of existence that can be detected by the validation process.

In order to prevent elements from expiring prior to reaching the end of the needed validity period as defined by the business application, it is strongly recommended that Client/APPs make provisions for timely augmentation of signatures and seals.

Independently of the aforementioned provisions, the certSIGN validation service tries to

obtain proof data online as needed, in particular when stored elements are missing or expired in the signed data object at validation time, for the purpose of determining the signature's overall diagnostics.
It has however to be kept in mind that online proof data may not be suitable to cope with situations that cryptographic algorithms on crucial elements of a signed data object are no longer eligible. In those particular cases, timely augmentation becomes inevitable for ensuring sufficient resilience with regard to the required long-term validity of signatures and seals.

BSP (k): ARCHIVING

The present policy imposes no specific archiving requirements for signatures. The longevity of the latter must be tailored by the Client/APP so that it is sufficient for the considered use case.
If needed, archiving of the signature has to be taken into account by the Client/APP, which may delegate it to the signatory with respect to its own signature policy or terms of use.
The certSIGN validation service can only consider evidences that are provided in a validation request. Consequently, the Client/APP must make provisions for suitable longevity of to be validated signatures in a timely manner in order to ensure its resilience and availability at the time of validation.
Nevertheless, the certSIGN validation service transaction logs are backed up in order to provide complementary evidence concerning the supplied service, archived for 10 (ten) years and accessible for use during legal proceedings.
The following types of evidence can be revealed by the certSIGN transaction log:

- The record creation time which is synchronized with a trustworthy accurate time source
- The unique identifier of the requesting Client/APP
- The entire validation report comprising the relevant transactional information
- Whether the request was successful

4.3 BSPs Mainly Related to the Actors Involved in Creating /Augmenting /Validating Signatures

BSP (l): IDENTITY (AND ROLES/ATTRIBUTES) OF THE SIGNERS

The validation service reveals the signatory identity, which can be taken into account by the business application for making workflow decisions at its own discretion. The present validation policy contains no requirement concerning the signatory's role.

BSP (m): LEVEL OF ASSURANCE REQUIRED FOR THE AUTHENTICATION OF THE SIGNATORY

The signatory level of assurance is implied by performing validation based on the trust anchors published in the EU Trusted Lists.
The certSIGN validation service reveals the legal type of a signature, which ensures the corresponding minimum assurance level.

BSP (n): SIGNATURE CREATION DEVICES

Upon successful validation of a signature, the certSIGN validation service implicitly reveals by detection of the legal type of a signature, whether a **Qualified Signature Creation Device** (QSCD) has been used by the signatory. The business application can use this information in order to make workflow decisions on its own discretion.

4.4 Other BSPs

BSP (o): OTHER INFORMATION TO BE ASSOCIATED WITH THE SIGNATURE

No specific requirement

BSP (p): CRYPTOGRAPHIC SUITES

Unless otherwise specified in the configuration of the service for the Client/APP, the eligible cryptographic suites for signature validation are taken from ETSI TS 119 312 – "Electronic Signatures and Infrastructures (ESI); Cryptographic suites". The signature validation report will however not indicate whether the algorithm and key lengths were still trustworthy at the time of use.

BSP (q): TECHNOLOGICAL ENVIRONMENT

No specific requirement.

5 Appendix 2 – Qualified Validation policies- QSigSeal Validation parameters

According to ETSI TS 119 172-1 Chapter 4 Signature policies and signature policy document: „the signature policy shall be expressed under the form of a signature policy statement summary established on the basis of table A.1 from annex A".

Name and identifier of the validation policy authority: **Policies and Procedures Management Body** (see chapter 1.4.1 above)

5.1 Default – PadES validation policy

Name and identifier of the validation policy: **certSIGN QVal** – „certSIGN QVAL default_policy" - OID: **1.3.6.1.4.1.25017.4.2.1.2**
Identifier of the concerned validation(s) in the concerned validation workflow: **Qualified Signature/Seal Validation**

BSP	BSP Title	Business statement summary	Technical statement counterpart
BSP(a)	**Workflow (sequencing & timing) of signatures**		
	The present validation policy address validation of the advanced electronic signatures and qualified electronic signatures comprising possible timestamps and proof-data extensions regarding a single instance or multiple instances of DTBS during a single transaction, while a single report is returned by the service after a successfully performed validation. certSIGN validation service may be used by a Client/APP to implement business workflows comprising multiple transactions; in such a case, each single transaction within the Client/APP workflow will be performed according to one of the present policies depending on the chosen validation mode. The default workflow is sequenced according to ETSI TS 119 102-1 V1.2.1.	Workflow at signature moment = irrelevant
			Multiple signatures = serial
			Sync all with a fixed moment = no
			Sync validation time with signature moment = yes
			With time stamp = specific per signature's level
			Level of Trust (LoA) = specific per signature's level
BSP(b)	**Data to be signed (DTBS)**		
	The Client/APP is responsible for the content and the correct formatting of the data to be validated with respect to applicable standards. In particular, it must ensure that the data to be validated does not contain malicious code or scripts that could alter the data to be validated or damage certSIGN services. In particular, the format of an SD can be only PDF. certSIGN validation service guarantees the confidentiality of an SD according to applicable laws on privacy and Romanian laws. certSIGN particularly and immediately erases all copies of a received SD, if any, from its servers after having performed a requested transaction. certSIGN validation service applies antivirus/malware scanning procedures before applying the signature validation process.	MimeType = application/pdf
			Data format & structure = cf. ETSI EN 319 142-1
			Structured objects = no
BSP(c)	**The relationship between signed data and signature(s)**		

BSP	BSP Title	Business statement summary	Technical statement counterpart
	The relationship between signed data and signature(s) specifically depends on the signature profile. The supported signature profiles/levels are: 1. B-B (basic signature) 2. B-T (signature with time) 3. B-LT (signature with long-term validation material) 4. B-LTA (Signatures providing long-term availability and integrity of validation material) The validation report will indicate the corresponding profile/level found for examined signatures and involved timestamps in the event that they can be validated successfully.		DTBSCardinality = 1
			Multiple signature validation = integral – all ok
			SigDTBSRelativePosition = EnvelopedSig
			SigLevels: http://uri.etsi.org/ades/191x2/level/baseline/B-B http://uri.etsi.org/ades/191x2/level/baseline/B-T http://uri.etsi.org/ades/191x2/level/baseline/B-LT http://uri.etsi.org/ades/191x2/level/baseline/B-LTA
			SigFormats: http://www.etsi.org/19142/v.1.1.1
BSP(d)	**Targeted community**		
	There is no specific targeted community to be addressedother than the mentions from section BSP (d) of Appendix 1.		Specific target group = no
			Exclusions = no
BSP(e)	**Allocation of responsibility for signature validation and augmentation**		
	certSIGN validation service has the responsibility of validation process validating existing signatures on the DTBS and is not responsible for augumentation of the signatures. Should the DTBS contain an invalid signature, that information is indicated in the result supplied by the service. certSIGN will NOT abort the validation process due to an invalid signature being contained in the DTBS.		
BSP(f)	**Legal type of the signatures**		
	In addition to advanced electronic signatures, the certSIGN validation service supports validation for all legal types of qualified electronic signatures for legal persons (in the case qualified seals) or for physical persons (qualified signatures) that act on their own behalf or on behalf of a legal person: • Qualified electronic signatures supported by an X.509 v3 qualified certificate; The legal type of a signature is indicated in the validation report when it can be validated successfully.		SCD devices level = SCD/QSCD
			Trust anchors = EU Trusted Lists
			Certificate type level = ESig/ESeal/QESig/QESeal
BSP(g)	**Commitment assumed by the signer**		
	The certSIGN validation service processes any commitment type found within the signature if it is according with section 5.2.3 of ETSI EN 319 122-1. The certSIGN validation service can reveal the commitment type when associated with a given signature for being taken into account by the business application.		Commitment type syntax = cf. ETSI EN 319 122-1.

BSP	BSP Title	Business statement summary	Technical statement counterpart
	The validation service does not interpret a commitment type that is associated with a signature.		
BSP(h)	**Level of assurance on timing evidences**		
	As specified in section BSP(h) from Appendix 1. Claimed by signatory for the basic level, timestamp for higher levels.		Time evidence proves = TSP time stamp cf. RFC 3161
			Level of the time stamp token = NotQualified/Qualified
			SigningCertTrustConditions: EU Trusted Lists
BSP(i)	**Formalities of signing**		
	The certSIGN validation service applies the validation procedures to the PDF document provided as input by the user. The certSIGN validation service reveals in the final status report the associated signature attributes.		
BSP(j)	**Longevity and resilience to change**		
	According to signature level described in section BSP(j) from Appendix 1.		
BSP(k)	**Archival**		
	The present policy imposes no specific archiving requirements for signatures. The longevity of the latter must be tailored by the Client/APP so that it is sufficient for the considered use case.		
BSP(l)	**Identity (and roles/attributes) of the signers**		
	The validation service may identifies and reveals the identity and type of the signer using the signer's certificate properties. The present validation policy contains no requirement concerning the signatory's role. (		
BSP(m)	**Level of assurance required for the authentication of the signer**		
	The signatory level of assurance is implied by performing validation based on the trust anchors published in the EU Trusted Lists.. The certSIGN validation service will indicate in the final status report the type of the signer's certificate (qualified or not-qualified) and the list of the revocation info used by the service to validate the certificate.		TrustAnchors = EU Trusted Lists
			ServiceTypes = qualified/not-qualified
			ServiceStatuses = granted/ recognisedatnationallevel/ recognisedatnationallevel/ setbynationallaw
			RevocationCheckingConstraints = eitherCheck
BSP(n)	**Signature creation devices**		
	Upon successful validation of a signature, the certSIGN validation service implicitly reveals by detection of the legal type of a signature, whether a Qualified Signature Creation Device (QSCD) has been used by the signatory. The business application can use this information in order to make workflow decisions on its own discretion.		
BSP(o)	**Other information to be associated with the signature**		
	No specific requirement.		Geographic location = no
			Signing time = time stamp/signatory claimed time

BSP	BSP Title	Business statement summary	Technical statement counterpart
BSP(p)	**Cryptographic suites**		
	Unless otherwise specified in the configuration of the service for the Client/APP, the eligible cryptographic suites for signature validation are taken from ETSI TS 119 312 – "Electronic Signatures and Infrastructures (ESI); Cryptographic suites". The signature validation report will however not indicate whether the algorithm and key lengths were still trustworthy at the time of use.		Cryptographic suites = cf. ETSI TS 119 312
BSP(q)	**Technological environment**		
	No specific requirements		Environment type = in Data Center

The „default_policy" do not apply any other specific constraints.

5.2 CAdES validation policy

Name and identifier of the validation policy: **certSIGN QVal CAdES** – „certSIGN QVAL CAdES_policy" - OID: **1.3.6.1.4.1.25017.4.2.2.1**
Identifier of the concerned validation(s) in the concerned validation workflow: **Qualified Signature/Seal Validation**

BSP	BSP Title	Business statement summary	Technical statement counterpart
BSP(a)	**Workflow (sequencing & timing) of signatures**		
	The present validation policy address validation of the advanced electronic signatures and qualified electronic signatures comprising possible timestamps and proof-data extensions regarding a single instance or multiple instances of DTBS during a single transaction, while a single report is returned by the service after a successfully performed validation. certSIGN validation service may be used by a Client/APP to implement business workflows comprising multiple transactions; in such a case, each single transaction within the Client/APP workflow will be performed according to one of the present policies depending on the chosen validation mode. The default workflow is sequenced according to ETSI TS 119 102-1 V1.2.1.	Workflow at signature moment = irrelevant
			Multiple signatures = serial
			Sync all with a fixed moment = no
			Sync validation time with signature moment = yes
			With time stamp = specific per signature's level
			Level of Trust (LoA) = specific per signature's level
BSP(b)	**Data to be signed (DTBS)**		
	The Client/APP is responsible for the content and the correct formatting of the data to be validated with respect to applicable standards. In particular, it must ensure that the data to be validated does not contain malicious code or scripts that could alter the data to be validated or damage certSIGN services.		MimeType = application/pdf
			Data format & structure = cf. ETSI EN 319 122-1
			Structured objects = no

BSP	BSP Title	Business statement summary	Technical statement counterpart
	certSIGN validation service guarantees the confidentiality of an SD according to applicable laws on privacy and Romanian laws. certSIGN particularly and immediately erases all copies of a received SD, if any, from its servers after having performed a requested transaction. certSIGN validation service applies antivirus/malware scanning procedures before applying the signature validation process.		
BSP(c)	**The relationship between signed data and signature(s)**		
	The relationship between signed data and signature(s) specifically depends on the signature profile. The supported signature profiles/levels are: 1. B-B (basic signature) 2. B-T (signature with time) 3. B-LT (signature with long-term validation material) 4. B-LTA (Signatures providing long-term availability and integrity of validation material) The validation report will indicate the corresponding profile/level found for examined signatures and involved timestamps in the event that they can be validated successfully.		DTBSCardinality = 1
			Multiple signature validation = no
			SigDTBSRelativePosition = EnvelopedSig
			SigLevels: http://uri.etsi.org/ades/191x2/level/baseline/B-B http://uri.etsi.org/ades/191x2/level/baseline/B-T http://uri.etsi.org/ades/191x2/level/baseline/B-LT http://uri.etsi.org/ades/191x2/level/baseline/B-LTA
			SigFormats: http://www.etsi.org/19122/v.1.1.1
BSP(d)	**Targeted community**		
	There is no specific targeted community to be addressedother than the mentions from section BSP (d) of Appendix 1.		Specific target group = no
			Exclusions = no
BSP(e)	**Allocation of responsibility for signature validation and augmentation**		
	certSIGN validation service has the responsibility of validation process validating existing signatures on the DTBS and is not responsible for augumentation of the signatures. Should the DTBS contain an invalid signature, that information is indicated in the result supplied by the service. certSIGN will NOT abort the validation process due to an invalid signature being contained in the DTBS.		
BSP(f)	**Legal type of the signatures**		
	In addition to advanced electronic signatures, the certSIGN validation service supports validation for all legal types of qualified electronic signatures for legal persons (in the case qualified seals) or for physical persons (qualified signatures) that act on their own behalf or on behalf of a legal person: • Qualified electronic signatures supported by an X.509 v3 qualified certificate; The legal type of a signature is indicated in the validation report when it can be validated successfully.		SCD devices level = SCD/QSCD
			Trust anchors = EU Trusted Lists
			Certificate type level = ESig/ESeal/QESig/QESeal

BSP	BSP Title	Business statement summary	Technical statement counterpart
BSP(g)	**Commitment assumed by the signer**		
	The certSIGN validation service processes any commitment type found within the signature if it is according with section 5.2.3 of ETSI EN 319 122-1. The certSIGN validation service can reveal the commitment type when associated with a given signature for being taken into account by the business application. The validation service does not interpret a commitment type that is associated with a signature.		Commitment type syntax = cf. ETSI EN 319 122-1.
BSP(h)	**Level of assurance on timing evidences**		
	As specified in section BSP(h) from Appendix 1. Claimed by signatory for the basic level, timestamp for higher levels.		Time evidence proves = TSP time stamp cf. RFC 3161 and signing time indication claimed by the signer
			Level of the time stamp token = NotQualified/Qualified
			SigningCertTrustConditions: EU Trusted Lists
BSP(i)	**Formalities of signing**		
	The certSIGN validation service applies the validation procedures to the SD provided as input by the user. The certSIGN validation service reveals in the final status report the associated signature attributes.		
BSP(j)	**Longevity and resilience to change**		
	According to signature level described in section BSP(j) from Appendix 1.		
BSP(k)	**Archival**		
	The present policy imposes no specific archiving requirements for signatures. The longevity of the latter must be tailored by the Client/APP so that it is sufficient for the considered use case.		
BSP(l)	**Identity (and roles/attributes) of the signers**		
	The validation service may identifies and reveals the identity and type of the signer using the signer's certificate properties. The present validation policy contains no requirement concerning the signatory's role. (		
BSP(m)	**Level of assurance required for the authentication of the signer**		
	The signatory level of assurance is implied by performing validation based on the trust anchors published in the EU Trusted Lists. The certSIGN validation service will indicate in the final status report the type of the signer's certificate (qualified or not-qualified) and the list of the revocation info used by the service to validate the certificate.		TrustAnchors = EU Trusted Lists
			ServiceTypes = qualified/not-qualified
			ServiceStatuses = granted/ recognisedatnationallevel/ recognisedatnationallevel/ setbynationallaw
			RevocationCheckingConstraints = eitherCheck
BSP(n)	**Signature creation devices**		

BSP	BSP Title	Business statement summary	Technical statement counterpart
	Upon successful validation of a signature, the certSIGN validation service implicitly reveals by detection of the legal type of a signature, whether a Qualified Signature Creation Device (QSCD) has been used by the signatory. The business application can use this information in order to make workflow decisions on its own discretion.		
BSP(o)	**Other information to be associated with the signature**		
	No specific requirement.		Geographic location = no
			Signing time = time stamp/signatory claimed time
BSP(p)	**Cryptographic suites**		
	Unless otherwise specified in the configuration of the service for the Client/APP, the eligible cryptographic suites for signature validation are taken from ETSI TS 119 312 – "Electronic Signatures and Infrastructures (ESI); Cryptographic suites". The signature validation report will however not indicate whether the algorithm and key lengths were still trustworthy at the time of use.		Cryptographic suites = cf. ETSI TS 119 312
BSP(q)	**Technological environment**		
	No specific requirements		Environment type = in Data Center

The „CAdES validation policy" do not apply any other specific constraints.

6 Appendix 3 – Tests descriptions

6.1 Introduction

This appendix describes a series of tests applied by Certsign SA (certSIGN) to validate the functionality provided by the Qualified Signature/Signature Validation Service.
In total, there are more than 500 tests, both positive and negative, designed to cover the widest possible range of cases. certSIGN also participated in the regular ETSI Plugtests event held at the end of 2023. Thus, a wide variety of tests were generated using files generated by external actors, namely other TSP companies, through which we validated the interoperability of the Qualified Signature/Signature Validation Service across EU member countries.

6.2 Tests

The following is a summary list of the main tests used to demonstrate the correct implementation of the validation service.

Test name	Description	Expected Result	Achieved Result	Observations
1_1_Adobe_B	B-B profile validation testing	TOTAL-PASSED	TOTAL-PASSED	
1_2_Adobe_BT	B-T profile validation testing	TOTAL-PASSED	TOTAL-PASSED	
1_3_1_Adobe_LT_Partial_ByteRange	Validation testing of a valid signature not covering the whole document	TOTAL-PASSED	TOTAL-PASSED	
2_Adobe_OnlyTimestamp	Testing document signed only with a Document Timestamp.	TOTAL-PASSED	TOTAL-PASSED	
4_1_FlowSign_LT	B-LT profile validation testing	TOTAL-PASSED	TOTAL-PASSED	
4_2_FlowSign_LTA	B-LTA profile validation testing	TOTAL-PASSED	TOTAL-PASSED	
5_1_FlowSign_LT_LT	Validation testing of signed document with two valid LT level signatures	TOTAL-PASSED	TOTAL-PASSED	
11_OneSignature_OneEmptyField	Validation testing of a signed document containing one signature and one blank signature field	TOTAL-PASSED	TOTAL-PASSED	
7_6_Adobe_LTA_LTA	Validation testing of a signed document with two valid LTA-level signatures	TOTAL-PASSED	TOTAL-PASSED	
8_1_Adobe_BT_B	Validation testing of a document with two signatures, the first of which is of level B-T and the second of level B-B.	TOTAL-PASSED	TOTAL-PASSED	
2_Unsigned	Document validation test without signature.	TOTAL-FAILED FORMAT_FAILURE	TOTAL-FAILED FORMAT_FAILURE	
3_SelfSigned	Validation testing signed document with self-signed certificate that is not trusted.	INDETERMINATE NO_CERTIFICATE_CHAIN_FOUND	INDETERMINATE NO_CERTIFICATE_CHAIN_FOUND	
MissingAttrs_3	Validation testing signed document with B-B level signature whose certificate was valid for 1 year. In addition, the 'signing-certificate' attribute is missing.	INDETERMINATE NO_POE	INDETERMINATE NO_POE	
MissingAttrs_7	Validation test signed document whose signature is missing the 'message-digest' and 'signed-certificate' attributes.	INDETERMINATE SIG_CONSTRAINTS_FAILURE	INDETERMINATE SIG_CONSTRAINTS_FAILURE	