DIGITALSIGN - CERTIFICADORA DIGITAL, SA.

SIGNATURE VALIDATION SERVICE POLICY AND PRACTICE STATEMENTS

VERSION 1.0 – 29/09/2022

[LANGUAGE: ENGLISH]

VERSION HISTORY

Date	Edition n.º	Content
29/09/2022	1.0	Initial draft

RELATED DOCUMENTS

Document Details	Author(s)
Certification Practice Statement	DigitalSign

AUTHORIZATIONS

Created by	Approved by
	

LEGAL NOTICE

Any question or request for information regarding the content of this document should be directed to suporte@digitalsign.pt.

CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

The present document is entitled "Signature Validation Service Policy and Practice Statements". The purpose of the Policy and the Practice Statement is to meet the general requirements in order to provide trust and confidence in electronic transactions including, amongst others, the generally applicable requirements from Regulation (EU) No. 910/2014 establishing a legal framework for electronic signature and electronic seal, including their validation. Therefore, the present document is to define the practices and procedures used to support the validation rules regarding Qualified Signature and Qualified Seal in conformity with Regulation (EU) No 910/2014, European Standards – ETSI, Legal acts of Portugal and guarantees that this service:

- Applies operational procedures and security management procedures that exclude any possibility for manipulation of the data and the status of the validated certificates;
- Checks the validity of the electronic signature/seal according to the requirements of Article 33 of Regulation (EU) No. 910/2014;
- Checks the status of the certificates in accordance with applicable recommendations (CRLs and/or OCSP);
- Validates qualified certificates and electronic signatures/seals;
- Fulfils the technical procedures for validation of signatures according to the requirements of ETSI TS 319 102-1 and ETSI TS 119 172-4;
- DigitalSign (as a Qualified Signature Validation Service Provider - QSVSP) can provide additional information about the signature/seal, e.g. if it is an advanced electronic signature/seal based on a qualified certificate;
- In order to guarantee the proper functioning of the validation service, DigitalSign tests each change in the validation service functionality and the tests are saved in the internal documentation of DigitalSign. The tests are subject to verification and statements;
- The validation report is authenticated with the electronic seal of DigitalSign;
- The validation report may be provided to the relying party automatically in accordance with ETSI TS 119 442 and ETSI TS 119 102-2;
- The validation report may be presented to the user through a web page within a TLS session supported by a certificate issued by the certification authority in a form convenient for them;
- The validation report contains a qualified timestamp which is in line with Regulation (EU) No. 910/2014;
- DigitalSign checks the hash computation based on which the document was signed. The establishment of the link between the signed document and the signature is in line with the requirements of Regulation (EU) No. 910/2014;

- The signature (OID) validation policy is in line with ETSI TS 119 172-4 and unambiguously states that the signature is qualified according to Regulation (EU) No. 910/2014;
- The validation report allows the relying party to be confident in the security of the signature/seal. There is information that the certificate has been issued by a Qualified Trust Service Provider and that it has been valid as of the moment of being signed. The data about the signature validation correspond to the data provided by the relying party. The use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing. The electronic seal is created by an electronic sealing device. The integrity of the data signed is not threatened.

Furthermore, the present document has been prepared in accordance with current Portuguese legislation and European legislation and standards for the provision of qualified trust services. Therefore, this document is compliant to the Annex A of ETSI TS 119 441 V1.1.1 (2018-08).

1.1.1. NORMATIVE REFERENCES

- **Regulation (EU) No 910/2014** of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- **ETSI TR 119 001** "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations";
- **ETSI TS 119 102-2** "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report";
- **ETSI EN 319 122-1** "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures";
- **ETSI EN 319 122-2** "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures";
- **ETSI EN 319 132-1** "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures";
- **ETSI EN 319 132-2** "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures";
- **ETSI EN 319 142-1** "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures";
- **ETSI EN 319 142-2** "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles";
- **ETSI TS 119 172-1** "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents";

- **ETSI TS 119 172-4** "Electronic Signatures and Infrastructures (ESI); Signature policies; Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted Lists";
- **ETSI TS 119 442** "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services";
- **ETSI EN 319 403** "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers";
- **ETSI TS 119 312** "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites";
- **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);
- **ETSI EN 319 411-1** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements";
- **ETSI EN 319 411-2** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates";
- **ETSI EN 319 412-4** "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates";
- **ETSI TS 119 172-2** "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 2: XML format for signature policies";
- **ETSI TS 119 172-3** "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 3: ASN.1 format for signature policies";
- **IETF RFC 3647** "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

1.1.2. QTSP IDENTIFICATION

DigitalSign – Certificadora Digital, S.A.
Largo Pe. Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira, Guimarães
Portugal
E-mail: geral@digitalsign.pt
Support Phone: +351 253 560 650

1.1.3. SUPPORTED SIGNATURE VALIDATION SERVICE POLICY

The Qualified Signature and Seal Validation Service Policy is identified with a registered formal object identifier (OID) **1.3.6.1.4.1.25596.5.1.1**

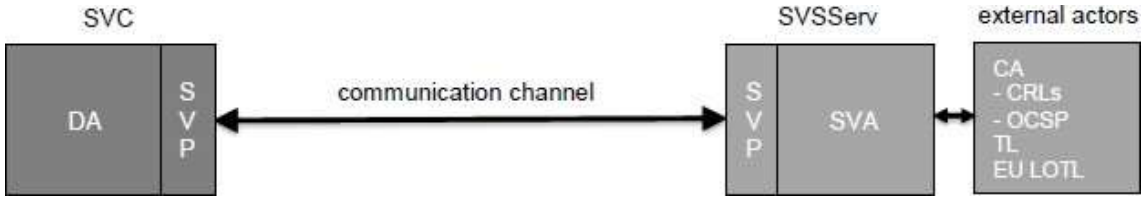
1.2. SIGNATURE VALIDATION SERVICE COMPONENTS

1.2.1. SVS ACTORS

- **Signature Validation Client (SVC)**
  A software component that provides user interface for Driving Application used by DigitalSign Service Subscribers.
- **Driving Application (DA)**
  Application which provides signature validation functionality to Signature Validation Client.
- **Signature Validation Service Protocol (SVP)**
  Secure communication channel for exchanging information with Signature Validation Service Server (SVSServ).
- **Signature Validation Service Server (SVSServ)**
  The component that implements the signature validation protocol on the SVSP's side.
- **Signature Validation Application (SVA)**
  A software component that is responsible for signature validation, which implements the validation algorithm and creates a signature validation report.
- **External Actors**
  Other trust sources - Certification Authorities, Time-stamping authorities, European Trusted List providers, European Commission providing the list of Trusted Lists which are called to fulfil its purpose.

1.2.2. SERVICE ARCHITECTURE

Please find below a simplified architecture and the involved actors:



1.3. DEFINITIONS AND ABBREVIATIONS

1.3.1. DEFINITIONS

- **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).
- **Information Security Management System:** certified Information Security Management System according to ISO/IEC 27001.
- **Qualified Trust Service Provider:** An entity which provides one or more Qualified Trust Services and is granted the qualified status by the Supervisory Body.
- **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 Regulation in the territory of that member state.
- **DigitalSign Signature Validation Practice Statement:** A statement of the practices that DigitalSign employs in providing Qualified Trust Services.
- **Signature Validation Service:** Trust Service for Signature and/or Seal Validation.
- **Signature Validation Application**: A software component that is responsible for signature validation, which implements the validation algorithm and creates a signature validation report.
- **Acceptance of the signature**: technical verification to be carried out on the signature itself or on the attributes of the signature.
- **Signature validation client**: software component that implements the signature validation protocol to the user.
- **Validation data**: data that is used to validate an electronic signature.
- **Signature validation status**: one of the following indications: TOTAL-PASSED, TOTAL-FAILED or UNDETERMINED.
- **Signature validation report**: full validation report prepared by the signature validation application. It allows you to inspect the details of the assessments taken during the validation and to investigate the status indications detailed by the validation application.
- **Signature validation policy**: set of signature validation constraints that are processed by the validation application that determine the result of the validation (PASS, FAIL, or UNDETERMINED).

- **Qualified validation service provider**: SVSP that provides a qualified validation service for electronic seals and/or electronic signatures.
- **Qualified validation service for qualified electronic seals**: as specified in Regulation (EU) No. 910/2014, Article 40.
- **Qualified validation service for qualified electronic signatures**: as specified in Regulation (EU) No.910/2014, Article 33.
- **Signature validation service server**: computer equipment that implements the signature validation protocol and processes the signature/electronic seal validation.
- **Subscriber:** it corresponds to the client, natural or legal person, who hires the validation service and submits signatures and/or electronic seals to validation.
- **User**: application or human being that interacts with a signature validation client.
- **Validation**: verification process and confirmation of the validity of a certificate or an electronic signature.

1.3.2. ABBREVIATIONS

DA: Driving Application
PoE: Proof of Existence
QES: Qualified Electronic Signature or Qualified Electronic Seal
AdES: Advanced Electronic Signature
AdES/QC: Advanced Electronic Signature created with a Qualified Certificate
(Q)SCD: Qualified Signature Creation Device
QSVSP: Qualified Signature Validation Service Provider
SD: Signer's Document
SDO: Signed Data Object
SDR: Signed Document Representation
SVA: Signature Validation Application
SVP: Signature Validation Protocol
SVR: Signature Validation Report
SVSP: Signature Validation Service Provider
SVSServ: Signature Validation Service Server
TSA: Time stamping Authority
VPR: Signature Validation Process
OID: Object Identifier
PKI: Public Key Infrastructure
OCSP: Online Certificate Status Protocol
CRL: Certificate Revocation List
HSM: Hardware Security Module

1.4. POLICIES AND PRACTICES

1.4.1. ORGANIZATION ADMINISTRATING THE QTSP DOCUMENTATION

DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal

1.4.2. CONTACT PERSON

Álvaro Matos
DigitalSign – Certificadora Digital, SA.
Largo Padre Bernardino Ribeiro Fernandes, 26
4835-489 Nespereira – Guimarães
Portugal
Email: svs@digitalsign.pt
Phone: +351 253560650
Fax: +351 253560639

1.4.3. QTSP (PUBLIC) DOCUMENTATION APPLICABILITY

DigitalSign's public documentation which is related to the provision of the qualified validation service has been made available to all users and is published on the internet on https://pki.digitalsign.pt/.

Present policy and practice statement

The management group of this policy evaluates the compliance and internal applicability of this Signature Validation Service Practice statement, submitting it to the approval of DigitalSign's Administration, which is the competent body to determine its suitability to the applicable legislation.

The internal approval of this documentation and following fixes and/or updates are made by DigitalSign's Administration. After internal approval, should be assessed their compliance, as described in the previous paragraph. Corrections and/or updates shall be published in the form of new versions of the Signature Validation Service Practice statement, replacing any previous version.

Policy OID is referred in section 1.1.3 of this document.

Terms and conditions

DigitalSign has its terms and conditions available on https://pki.digitalsign.pt/.

Risk assessment and Information security policy

DigitalSign has an information security management system based on the standard ISO/IEC 27001, ensuring that facilities, procedures, personnel, equipment and products comply with all regulatory and safety requirements applicable to the exercise of its activity. Thus, it uses reliable systems and products, protected from modification, performs planned security audits and prepares reports of

incidents caused by possible security or operation failures, triggering the respective corrective actions in a timely manner.
Ensures that the procedures used to ensure operational safety levels, physical and systems, in accordance with the adopted standards, are documented, implemented and updated, and maintains an inventory of assets with the respective classification, in order to characterize their protection needs.

2. TRUST SERVICE MANAGEMENT AND OPERATION

2.1. INTERNAL ORGANIZATION AND ORGANIZATION RELIABILITY

DigitalSign conducts its operations through certification and registration authorities in line with the adopted policies and practices. The contact information of the certification and registration Authorities is available on the website of DigitalSign. In order to achieve reliability and security in its operations related to the provision of trust services, DigitalSign applies the requirements specified in ETSI EN 319 401, including:

- DigitalSign guarantees high level of security and reliability of its operations;
- DigitalSign offers its Qualified Trust Services under non-discriminatory practices;
- DigitalSign ensures that all requirements defined in ISO/IEC 27001 Statement of Applicability and this Practice Statement are implemented and remain applicable to the Qualified Trust Services provided;
- DigitalSign complies with all legal obligations applicable to the provisioning of its Qualified Trust Services;
- DigitalSign fulfils general security requirements set out in article 19 of the eIDAS Regulation as further developed in ETSI EN 319 401;
- In relation to the validation of Qualified Trust Services, DigitalSign provides validation of (Qualified) Electronic Signatures and Seals in accordance with article 33 of the eIDAS Regulation and relevant sections of ETSI TS 119 102 Electronic Signatures and Infrastructures;
- The provision of Qualified Trust Services is subject to an external audit performed at least every 12 months by a Conformity Assessment Body (CAB) and the qualified status is supervised by GNS (Gabinete Nacional de Segurança), the Portuguese National Supervisory Body;
- Records concerning the operation of the Qualified 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;
- DigitalSign has the necessary financial stability and resources for operation in accordance with this document;
- DigitalSign 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.

2.1.1. SEGREGATION OF DUTIES

DigitalSign has established and maintains a policy of strict control procedures to ensure segregation of duties, based on the responsibilities of each task, and ensuring that multiple Trusted Persons are required to perform sensitive tasks.

2.1.2. DIGITALSIGN'S LIABILITY

In accordance with Article 13 of the eIDAS Regulation, DigitalSign will only be liable in relation to the DigitalSign qualified validation service for damages caused intentionally or negligently due to a failure to comply with its obligations under the eIDAS Regulation.
Any conflicting obligations and the scopes of responsibility shall be severed in order to minimise any possibility for unlawful or unintentional change or misuse of the TSP's assets.

2.1.3. CONFIDENTIALITY

The DigitalSign Signature validation service guarantees the confidentiality of a signed document according to applicable European and national laws on privacy and data protection. DigitalSign particularly and immediately erases all copies of a received SD, if any, from its servers after having performed a requested transaction.

2.2. HUMAN RESOURCES

In conformity with our global CPS (Certificate Practice Statement), DigitalSign ensures:

- All members of the personnel staff that involved for the provision of the DigitalSign services are either employees of DigitalSign or authorised and qualified personnel of sub-contracting entities providing sub-contracted certification and/or time stamping component services;
- All members are subject to personnel and management practices that DigitalSign follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and related services;
- DigitalSign requires that staff try to be a Trusted Person, must provide evidence of background, qualifications, experience and clearance necessary to perform their possible liability tasks, competently and satisfactorily.
- DigitalSign acting as QTSP obtains a signed statement from each member of the staff on not having conflicting interests with the QTSP, on the preservation of confidentiality and the protection of personal data;
- DigitalSign ensures that all tasks, roles and responsibilities with respect to the DigitalSign trusted services are described in job descriptions and made available to the concerned personnel. These job descriptions are defined from the view point of segregation of duties and least privileges, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness;
- Personnel shall exercise administrative and management procedures and processes that are in line with the DigitalSign information security management procedures;
- Managerial personnel possess expertise in the field of electronic signature and related services, in risk assessment and information security as well as possess familiarity with security procedures for personnel with security responsibilities;

- Training and awareness-raising actions (internal and external);
- Periodic review of the Trusted Person Statute.

2.3. ASSET MANAGEMENT

DigitalSign ensures implementation and maintains appropriate level of protection to its assets and information systems. For this purpose, DigitalSign maintains an inventory of all information assets (both virtual and physical) and their owners, identifying their threats and assigning a classification for the protection requirements to those assets consistent with the risk analysis.

2.4. ACCESS CONTROL

In accordance with the information security policy, the DigitalSign's system access is limited to authorized individuals. In particular, DigitalSign ensures the following measures, among others:

- DigitalSign's personnel is identified and authenticated before using critical applications related to the service
- Use of firewalls to protect the internal network domains from unauthorized access including access by subscribers and third parties;
- Firewalls are configured to prevent all protocols and accesses not required for the operation of the QTSP;
- Constant monitoring of systems and recording of information security events;
- Existence of Antivirus protection – automated systems of virus detection and elimination;
- Separation of management flows for administrators and operators, according with the segregation of duties rule;
- Sensitive data are protected against being revealed through storage and restriction of access thereto for unauthorized users.

2.5. CRYPTOGRAPHIC CONTROLS

DigitalSign applies the requirements for cryptographic controls specified in clause 7.5 of ETSI EN 319 401. In addition, DigitalSign also applies the following particular requirements:

- The QSVSP seals the validation reports with a qualified certificate issued by the certification authority in accordance with ETSI EN 319 411-1 or ETSI EN 319 411-2;
- The private key of QSVSP used to authenticate the validation reports is stored and used in QSCD.

2.6. PHYSICAL AND ENVIRONMENTAL SECURITY

DigitalSign applies the requirements of clause 7.6 of ETSI EN 319 401 concerning the physical and environmental security. Physical access to DigitalSign offices & data centre facilities is appropriately restricted to authorized personnel, in conformity to our global CPS (Certification Practice Statement). Safeguard measures are in place to protect critical assets and ensure continuity.

- Elaboration and maintenance of a list of persons authorized to access the facilities where the servers and system equipment are located;
- Monitoring of entrances - all existing doors and installations have access control with an anti-passback system, not being allowed to leave a specific room without registration;
- Organization of the facilities structure in four security levels;
- Reinforcement of access control through the use of an identification proximity card and, in some cases, an additional need for biometric authentication (fingerprint reader) and application of the Two Men Rule. In particular, areas used to create and store cryptographic material enforce dual control, each through the use of two-factor authentication including biometrics;
- Existence of a CCTV system and armoured security doors;
- Existence of glass break detectors, movement and open/closed door sensors;
- Location of critic assets at level 4 of security equipment;
- Personnel without escort, including non-accredited staff or visitors are not allowed in such security areas;
- Realization of periodic inspections and updates.

2.7. OPERATION SECURITY

DigitalSign applies the requirements specified in clause 7.7 of ETSI EN 319 401 in order to ensure security of its operations, as per information security policy. DigitalSign uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

- DigitalSign employs a layered security approach for protection against malware;
- The integrity of the systems and information of DigitalSign are protected against viruses, malicious and unauthorised software;
- Backup copies are ensured for all DigitalSign online products and services provided for clients;
- Realization of event logging, protection of log information, administrator and operator logs, clock synchronization, as well as control of operational software, via the installation of software on operational systems;
- 24/7 monitoring on the infrastructure, network and security components;

Detailed descriptions of implemented operation security controls are available as internal document(s).

2.8. NETWORK SECURITY

DigitalSign ensures that network security controls (including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc.) are implemented in compliance with the standard ETSI EN 319 401, specifically with 7.8 clause.
Detailed descriptions of implemented network security controls are available as internal document(s).

2.9. INCIDENT MANAGEMENT

The management of security incidents and improvements is integrated within the overall operations model and the standard incident management procedures there. Incidents are logged into an internal tool and assigned based on their classification. Security and privacy incidents are also forwarded to the CISO or DPO respectively, to keep him/her informed, and take immediate appropriate action.
Detailed descriptions of implemented incident management controls are available as internal document(s).

2.10. COLLECTION OF EVIDENCE

DigitalSign applies the requirements specified in clause 7.10 of ETSI EN 319 401 with respect to collection of evidence.
In addition, the following particular requirements are applied:

- DigitalSign implements event logs, marked with the time of the event, to capture information needed for later proofs, including type of the event, the event success or failure and an identifier of the person and/or component at the origin for such an event;
- Any signature validation is logged. As a standard, DigitalSign does not log the identity of the user;
- The archived data are stored for a period of 7 years. After expiration of this period the archived data are destroyed;

As above mentioned, DigitalSign maintains records concerning the operation of the services in scope for the purposes of providing evidence of the correct operation of these 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. Such information is managed in line with DigitalSign Personal Data Protection Policy.

2.11. BUSINESS CONTINUITY MANAGEMENT

DigitalSign applies the requirements specified in clause 7.11 of ETSI EN 319 401 with respect to business continuity management.
DigitalSign establishes the necessary measures to ensure full and highly automated recovery of the DigitalSign certification and time stamping services in case of a disaster, corrupted servers, software or data.

A Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

2.12. QTSP TERMINATION AND TERMINATION PLANS

DigitalSign has up-to-date termination plan in accordance with clause 7.12 of ETSI EN 319 401.
DigitalSign has created a termination plan that deals with termination notification, subcontractor's management, information maintenance, private key destruction, termination phasing and updating of the termination plan procedure. DigitalSign has taken measure to ensure that the execution of the termination plan is executed in case of bankruptcy.

2.13. COMPLIANCE

DigitalSign applies the requirements specified in clause 7.13 of ETSI EN 319 401 in order to ensure compliance with the legal requirements.
In particular,

- DigitalSign guarantees that it operates in a legal and trustworthy manner and it provides evidence on how it meets the applicable legal requirements;
- The CPS and provision of DigitalSign PKI Services are compliant to relevant and applicable European and national laws;
- DigitalSign employs personnel with the required legal skills and has that fulfil the required roles in order to guard the correct implementation of legal requirements;
- DigitalSign ensures that appropriate technical and organisational measures are undertaken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data, guaranteeing that personal data are processed in accordance with Regulation (EU) No. 2016/679 (commonly, GDPR).

3. SIGNATURE VALIDATION SERVICE DESIGN

3.1. SIGNATURE VALIDATION PROCESS REQUIREMENTS

The validation process complies with ETSI TS 119 102-1. DigitalSign implements the algorithm specified in ETSI TS 119 102-1 by allowing alternative implementations provided that produce the same main status indication when given the same set of input information.
Therefore, DigitalSign complies with the following requirements:

- The signature validation policy is not limited to the minimum number of constraints required under clause 5.1.4.1 of ETSI TS 119 102-1;
- The validation process outputs a signature validation status indication and a signature validation report;

According to the algorithm specified in ETSI TS 119 102-1, the signature validation status can be:

Information entered in the report		Semantics
Indication	Report data	
TOTAL-PASSED	The validation process outputs the validated certificate chain, including the certificate for electronic signature/seal used in the validation process.	The qualified validation process of electronic signatures and seals results into TOTAL-PASSED based on the following considerations: • the cryptographic checks of the electronic signature/seal succeeded (including checks of hashes of individual data objects that have beensigned indirectly); • any constraints applicable to the signer's identity certification have been positively validated (i.e. the signing certificate has been found trustworthy); and • the electronic signature/seal has been positively validated against the validation constraints and hence is considered conformant to these constraints.
TOTAL-FAILED	The validation process outputs additional information to explain the TOTAL-FAILED indication for each of the validation constraints that have been taken into account and for which a negative result occurred.	The electronic signatures and seals validation process results into TOTAL-FAILED because the cryptographic checks of the electronic signature/seal failed (including checks of hashes of individual data objects that have been signed indirectly) or it has been proven that the generation of the signature/seal took place after its revocation.

INDETERMINATE	The validation process outputs Additional information to explain the INDETERMINATE indication and to help the verifiers to identify what data is missing to complete the validation process	The available information is insufficient for the validation process to ascertain the TOTAL-PASSED or TOTAL-FAILED status of the electronic signature/seal.

In addition to the main status, the signature validation report also includes a secondary indication with the following:

Information entered in the report			Semantics
Main indication	Sub-indication	Report data	
TOTAL-FAILED	FORMAT_FAILURE	The validation process provides the individual facts that have resulted in information available about the unsuccessful processing of an electronic signature/seal.	The electronic signature/seal is not compatible with the standards supported specified in this document to a level that prevents the cryptographic check to process it.
	HASH_FAILURE	The signature validation process provides an identifier that uniquely identifies the element within the signed data object/seal causing the failure in the form of the certificate for electronic signature/seal.	The qualified validation process of electronic signatures and seals results into TOTAL-FAILED because at least one hash of a signed data object that has been included in the signing process does not match the corresponding hash value in the signature/seal.
	SIG_CRYPTO_FAILURE	The validation process outputsthe certificate for electronic signature/seal used in the validation process.	The qualified validation process of electronic signatures and seals results into TOTAL-FAILED because the digital value of the signature could not be verified using the signer's public key in the certificate for electronic signature/seal.
	REVOKED	The validation process provides the following: • The certificate chain used in the validation process; • The time and, if available, the reason of revocation of the certificate for electronic	The qualified validation process of electronic signatures and seals results into a TOTAL-FAILED because: • the certificate for electronic signature/seal has been revoked; and • there is proof of existence (PoE) available that the time of the

Information entered in the report			Semantics
Main indication	Sub-indication	Report data	
		signature/seal. • CRL, if any, for which the revocation has been established.	signature/seal lies after the revocation time.
	EXPIRED	The process shall output: The validated certificate chain	The signature validation process results into TOTAL-FAILED because there is proof that the signature has been created after the expiration date (notAfter) of the signing certificate.
	NOT_YET_VALID		The signature validation process results into TOTAL-FAILED because there is proof that the signature was created before the issuance date (notBefore) of the signing certificate.
INDETERMINATE	SIG_CONSTRAINTS_FAILURE	The validation process provides multiple reasons that have resulted in unsuccessful validation	The qualified validation process of electronic signatures and seals results into INDETERMINATE because one or more attributes of the electronic signature/seal do not match the validation constraints.

Information entered in the report			Semantics
Main indication	Sub-indication	Report data	
	CRYPTO_CONSTRAINTS_FAILURE	The validation process provides identification of an electronic signature/seal or of a certificate generated using an algorithm or key size below the required cryptographic security level.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because at least one of the algorithms that have been used (for electronic signature/seal or the corresponding certificates) involved in the qualified validation of electronic signatures and seals, or the size of a keys used with such algorithms, are below the required cryptographic security level, and: • the electronic signature/seal and/or the corresponding certificates have been produced after the time up to which these algorithms/keys were considered secure (if such a time is known); and • the electronic signature/seal is not protected by a sufficiently strong timestamp applied before the time up to which the algorithm/key was considered secure (if such a time is known).
	POLICY_PROCESSING_ERROR	The validation process provides additional information on the reason.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the given formal policy file could not be processed for any reason (e.g. not accessible, not pursuable, digest mismatch,

Information entered in the report			Semantics
Main indication	Sub-indication	Report data	
	SIGNATURE_POLIY_NOT_AVAILABLE	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the document containing the details of the policy is not available.
	NO_SIGNING_CERTIFICATE_FOUND	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the certificate for electronic signature/seal cannot be identified.
	NO_CERTIFI CATE_CHAIN_FOUND	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because no certificate chain has been found for the identified certificate for electronic signature/seal.
	REVOKED_NO_POE	The validation process provides the following: • The certificate chain used in the validation process. • The time and the reason of revocation of the certificate for electronic signature/seal.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the corresponding certificates has been revoked during the validation. However, it may not be established whether the signature time lies before or after the revocation time.

Information entered in the report			Semantics
Main indication	Sub-indication	Report data	
	REVOKED_CA_NO_POE	The validation process provides the following: • The certificate chain which includes the revoked certification authority certificate; • The time and the reason of revocation of the certificate	The qualified validation process of electronic signatures and seals results into INDETERMINATE because at least one certificate chain was found but an intermediate certification authority is revoked.
	OUT_OF_BOUNDS_NOT_REVOKED		The signature validation process results into INDETERMINATE because the signing certificate is expired or not yet valid at the validation date/time and the Signature Validation Algorithm cannot ascertain that the signing time lies within the validity interval of the signing certificate. The certificate is known not to be revoked
	OUT_OF_BOUNDS_NO_POE	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the certificate is expired or not yet valid at the validation date/time and the SVA cannot ascertain that the signing time lies within the validity interval of the certificate.

Information entered in the report			Semantics
Main indication	Sub-indication	Report data	
	REVOCATION_OUT_OF_BOUNDS_NO_POE	The validation process shall provide the following: • The certificate chain used in the validation process. • The revocation information that is concerned by the failure.	The signature validation process results into INDETERMINATE because the signing certificate of the revocation information of the signature signing certificate is expired or not yet valid at the validation date/time and the Signature Validation Algorithm cannot ascertain that the revocation information issuance time lies within the validity interval of the signing certificate of that revocation information
	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	The validation process provides the following: Identification of the electronic signature/seal or the respective certificate that is produced using an unacceptable key size or algorithm that does not meet the required cryptographic security level.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because at least one of the algorithms that have been used in the electronic signature/seal or the respective certificates involved in their validation, or the size of a key used with such an algorithm, is below the required cryptographic security level, and there is no proof that the signature/seal or these certificates were produced before the time up to which this algorithm/key was considered secure.
	NO_POE	The validation process only identifies signatures/seals for which the proof of existence (PoEs) are missing. The validation process should provide additional information about the problem.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because there is no proof of existence (PoE) to ascertain that the signature/seal has been produced before some known compromising event (e.g. broken algorithm).

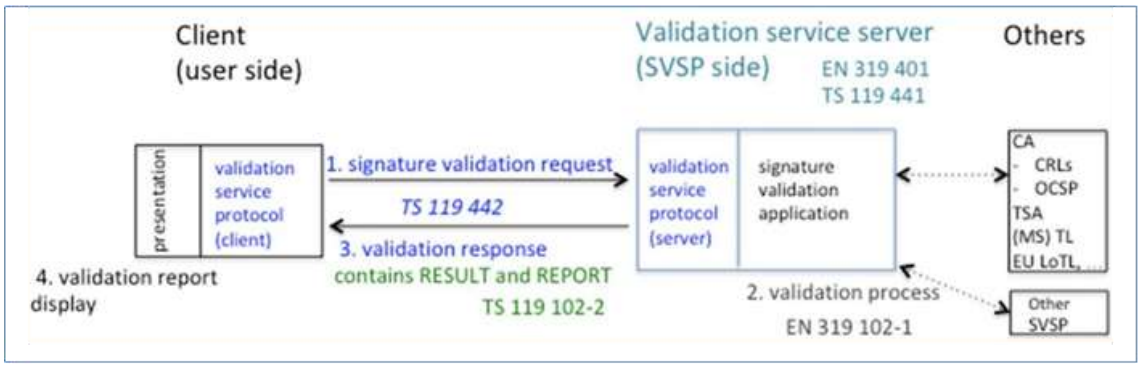
Information entered in the report			Semantics
Main indication	Sub-indication	Report data	
	TRY_LATER		The qualified validation process of electronic signatures and seals results into INDETERMINATE because not all constraints can be fulfilled using available information. However, the process may be possible if the validation uses additional revocation information that will be available at a later point of time.
	SIGNED_DATA_NOT_FOUND	The validation process provides the following: The identifier (e.g. an URI) of the signature/seal data that caused the failure.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the data about the signature/seal cannot be obtained.

- DigitalSign supports one signature validation policy for the signature validation application (SVA);
- The signature validation service (SVS) does not accept several sources of validation policy;
- The signature validation policy may not be ignored and replaced by signature validation rules in line with the protocol specified in ETSI TS 119 442, which supports diverse capabilities;
- The signature validation application (SVA) meets the requirements of clause 7.4 of ETSI TS 119 101 (SIA 1 through SIA 4);
- The validation process ensures that the signature validation policy that is used corresponds to the strategy defined in the SVS policy and/or the terms and conditions of use of the SVS. The strategy defined in the SVS policy and/or the terms and conditions of use of the SVS follows at least the next principles:
  - For one and the same input, the signature validation policy shall have the same output, by taking into account that the signature validation policy is part of the input;
  - SVS may accept different elements as a proof of existence for a signature.

3.1.1. VALIDATION PROCESS

Depending on the format of electronic signature/seal used, the service supports validation processes for baseline formats of the signature/seal and advanced formats (with added electronic timestamp or time verification data) as follows:

- Validation Process for Basic Signature/Seal - Baseline;
- Validation Process for Signatures/Seals with Time – Baseline + T;
- Validation Process for Signatures/Seals with Long-Term validation data – Baseline + LT.



The process comprises of the following steps:

Step 1. The client generates and submits a signature validation request. DigitalSign may use the protocols described in ETSI TS 119 442. The request contains the signer's document (s) (SD) and the signed data object(s) (SDO) used to sign them.

The validation constraints are defined in ETSI TS 119 102-1 and, according to this policy, DigitalSign restricts the validation only to the parameters described therein.

DigitalSign does not support signature validation policies provided by the user.

Step 2. SVSServ implements the validation process in accordance with ETSI TS 119 102-1.

Validation is performed by the QSVSP in accordance with the constraints set by the service itself. SVS applies the signature validation policy with a "default value".

Step 3. SVSServ prepares and sends a response for validation. DigitalSign may use the protocols described in ETSI TS 119 442. The response for confirmation of validation is input in the validation report. It bears the OID of the service policy and may build-in the OID of the signature validation policy applied. The validation report includes:

- The report is authenticated with a qualified electronic seal of DigitalSign.

Reports for each validation constraint:

- where the constraint has been processed, with the relevant result;
- where the constraint has not been processed, with an instruction that the constraint has been ignored or replaced, where appropriate.

Step 4. Presentation of the validation report.

3.1.2. VALIDATION CONSTRAINTS FOR ELECTRONICALLY SIGNED DOCUMENTS

The qualified validation service is controlled by a set of validation constraints. These constraints during operation are defined during the management of the service. Moreover, there may be constraints related to the used certificates for electronic signature/seal. The service supports specific constraints related to elements of the placed signature/seal, allowed cryptographic combinations and algorithms used as well as constraints within the qualified validation of electronic signatures and seals. There are constraints in the size of the electronically signed file accepted for signing. In addition, during the validation process a qualified time stamping service of DigitalSign is used, which has its own application policy.

3.1.3. VALIDATION CONSTRAINTS FOR CERTIFICATES FOR ELECTRONIC SIGNATURE/SEAL

The validation service supports the following validation constraints for the certificates for electronic signature/seal (ETSI TS 119 172-1, clause A.4.2.1, BSP (m), LoA on signer authentication):

Constraint(s)	Constraint value at qualified validation of electronic signatures and seals
(m) 1. **X509 CertificateValidationConstraints**: This set of constraints indicates the requirements in the course of validation of the certification chain in accordance with IETF RFC 5280 These constraints may be different for different certificate types (e.g. certificates issued to signer, to certification authorities, to OCSP responders, to CRL lists, electronic timestamps/TST). The semantic for a possible set of requirement values used to express such requirements is defined as follows: (m) 1.1 *SetOfTrustAnchors*: This constraint indicates a set of acceptable trust anchors (TAs) as a constraint for the validation process.	**European UnionTrusted List of Trust Service Providers** https://webgate.ec.europa.eu/tl-browser Other Trust Anchors
(m) 1.2 *CertificationPath*: This constraint indicates a certification path requiredto be used by the SVA for qualified validation of electronic signatures and seals. The certificate path is of length "n" from the trust anchor (TA) start down to the certificate of electronic signature/seal used in validating the signed object. This constraint can include the path or indicate the need for consideringthe path provided in the signature/seal, if any. ➢ (m) 1.3. *user-initial-policy-set:* According to IETF RFC 5280, clause 6.1.1 (c) ➢ (m) 1.4. *initial-policy-mapping-inhibit*: According to	None

IETF RFC 5280, clause 6.1.1 (e) ➢ (m) 1.5. *initial-explicit-policy*: According to IETF RFC 5280, clause 6.1.1 (f) ➢ (m) 1.6. *initial-any-policy-inhibit*: According to IETF RFC 5280, clause 6.1.1(g) ➢ (m) 1.7. *initial-permitted-subtrees*: According to IETF RFC 5280, clause 6.1.1(h) ➢ (m) 1.8. *initial-excluded-subtrees*: According to IETF RFC 5280, clause 6.1.1(i) ➢ (m) 1.9. *path-length-constraints*: This constraint concerns the number ofcertificates of the CA in the certification chain. ➢ (m) 1.10. *policy-constraints*: This constraint concerns the policy(ies) in the certificate for electronic signature/seal.	
(m) 2. **RevocationConstraints:** This set of constraints concerns the verification of the electronic signature/seal certificate validity status during the validation process. These constraints may be different for different certificate types for electronic signature/seal. The semantic for a possible/acceptable set of requirement values used to express such requirements is defined as follows: (m) 2.1. *RevocationCheckingConstraints:* This constraint concerns the requirements for checking the certificate for electronic/signature seal for revocation. Such constraints may specify if revocation checking is required ornot and if OCSP responses or issued CRLs have to be used. The semantic for a possible set of requirement values used to express such requirements is defined as follows: - ClrCheck: Checks are made against the current CRL; - OcspCheck: The revocation check is checked using OCSP IETF RFC 6960; - BothCheck: Both OCSP and CRL checks are carried out; - EitherCheck: Either OCSP or CRL checks are carried out; - NoCheck: No checks	EitherCheck

(m) 2.2. *RevocationFreshnessConstraints*: This constraint indicates time requirements on revocation information. The constraints may indicate the maximum accepted difference between the issuance date of the revocation status information of a certificate for electronic signature/seal and the time of validation, or require the SVA to only accept revocation information issued a certain time after the electronic signature/seal has been created/generated.	None
(m) 2.3. *RevocationInfoOnExpiredCerts*: This constraint mandates the certificatefor electronic signature/seal used in validating the signature/seal to be issuedby a CA that keeps the renewals of revoked certificates even after they have expired for a period exceeding a given lower bound.	None
3. LoAOnTSPPractices: This constraint indicates the required level of agreement (LoA) on the practices implemented by the TSP(s) having issued a certificate for electronic signature/seal to be validated during the certificate path validation process: EUQualifiedCertificateRequired EUQualifiedCertificateSigRequired EUQualifiedCertificateSealRequired 1	None

3.1.4. CRYPTOGRAPHIC SUITES CONSTRAINTS

The validation service supports cryptographic constraints related to the required algorithms and parameters. They are in accordance with the document ETSI TS 119 312 and fulfil the requirements of ETSI TS 119 172-1 (p)1. CryptographicSuitesConstraints: This constraint indicates requirements on algorithms and parameters used when creating electronic signatures/seals or used when validating signed/sealed objects included in the validation process (e.g. electronic signatures/seals, certificates, CRLs, OCSP responses, timestamps/TSTs).

3.1.5. SIGNATURE AND SEAL ELEMENTS CONSTRAINTS

The validation service supports constraints on the elements of qualified validation of electronic signatures and seals. According to the requirements of ETSI TS 119 172-1, these are:

Constraints	Constraint value at qualified validation of electronic signatures and seals

(b) 1. **ConstraintOnDTBS:** This constraint indicates requirements on the type of the data to be signed by the signer.	None
(b) 2. ContentRelatedConstraintsAsPartOfSignatureElements: This set of constraints indicates the required content related information elements under the form of signed or unsigned qualifying properties that are mandated to be present in electronic signatures/seals. The set includes: (b) 2.1 MandatedSignedQProperties-DataObjectFormat to require a specific format for the content being signed by the signer. (b) 2.2 *MandatedSignedQProperties-content-hints* to require specific information that describes the innermost signed content of a multi-layer message where one content is encapsulated in another for the content being signed by the signer. (b) 2.3 MandatedSignedQProperties-content-reference to require the incorporation of information on the way to link request and reply messages in an exchange between two parties, or the way such link has to be done, etc. (b) 2.4 MandatedSignedQProperties-content-identifier to require the presence of, and optionally a specific value for, an identifier that can be used later on in the signed qualifying property "content-reference" attribute.	None
(b)3. **DOTBSAsAWholeOrInParts:** This constraint indicates whether the whole data or only certain part(s) of it have to be signed. The semantic for a possible set of requirement values used to express such requirements is defined as follows: • Whole: the whole data has to be signed; • Parts: only certain part(s) of the data have to be signed. In this case additional information should be used to express which parts have to be signed.	None

3.2. SIGNATURE VALIDATION PROTOCOL REQUIREMENTS

The signature validation protocol used by DigitalSign conforms with ETSI TS 119 442. The signature validation response contains the OID of the SVS policy.

The communication channel between the client and the validation service transports the validation requests for the electronic signature in one direction and returns the response. It can be either synchronous or asynchronous. It covers the certification of QSVSP in order to avoid false data in the report and may support the client certification.

3.3. INTERFACES

The communication channel between the client and the QSVSP is secured by using a reliably protected channel under the HTTPS protocol and by using TLS 1.2 or higher. QSVSP guarantees that it can establish a secure channel with the client and keep the confidentiality of data.
The service uses HTTPS authentication through a server certificate/website authenticity certificate before an application or a client/browser, without requiring authentication on the part of the user. The service interface defines the validation interface for one or more documents signed with an electronic signature/seal.

3.3.1. COMMUNICATION CHANNEL

DigitalSign offers a secure communication channel and guarantees the confidentiality of the authentication process and users' personal data. DigitalSign allows secure user authentication.

3.3.2. QSVSP – OTHER TRUST SERVICE PROVIDERS

The signature verification status and the signature validation report may be affected by the practices, policies and agreements for compliance with other service providers that are outside the control of the SVSP. Other trust service providers that are in contact with DigitalSign (QSVSP) in its capacity as a qualified validation service providers may be time-stamping authorities (TSAs), other validation service providers (SVSP), other CRL providers, other certificate status validation providers (OCSP) to whom DigitalSign may forward requests, etc. The communication channel between the SVSP and other TSP is outside the scope of this document.

3.4. SIGNATURE VALIDATION REPORT

As a result of the automated processing, the service drafts a comprehensive report in PDF and XML format of the validation of the signature/seal, detailing the reasons for the provided status indications. The result of the validation process includes status of the results from the process of qualified validation of electronic signatures and seals. In addition, the extended report also includes the date and time of the validation status, as well as additional data.
The signature validation service (SVS) outputs a status indication and a validation report providing the details of the technical validation of each of the applicable constraints described in ETSI TS 119 102-1. The validation process is controlled by a set of validation constraints. Each validation constraint may originate from:

- the signature content itself, either directly (included in the signature attributes) or indirectly, i.e. by reference to an external document, provided either in a human readable and/or machine processable form.

Additional constraints may be provided by the DA to the SVA via set parameters. These constraints influence the validation process and the validation result, irrespective of where these constraints have been defined. Some of the constraints may be related to elements of the signature validation process that are widely implemented in applications and already have been standardised elsewhere, e.g. in IETF RFC 5280.

The following constraints are supported:

- Chain constraints, as defined in clause 5.1.4.2 of ETSI TS 119 102-1;
- Cryptographic constraints, as defined in clause 5.1.4.3 of ETSI TS 119 102-1;
- Signature elements constraints, as defined in clause 5.1.4.4 of ETSI TS 119 102-1.

The signature validation report may conform to the requirements of ETSI TS 119 102-2, as follows:

- it indicates one of the three status indications specified in ETSI TS 119 102-1: TOTAL-PASSED, TOTAL-FAILED or INDETERMINATE;
- it provides information about sub-indications as specified in ETSI TS 119 102-1;
- it may report any of the validation constraints that are processed, including all validation constraints implicitly by the implementation;
- it contains the signature validation policy identifier. This identifier is also present in the validation response where the protocol conforms to ETSI TS 119 442 and it is present in the validation report where it conforms to ETSI TS 119 102-2;
- it contains information about the signature validation process, where what has been defined under ETSI TS 119 102-2 may be followed with an identifier showing the validation process described under clause 5.3, 5.5 and 5.6.3 of ETSI TS 119 102-1 which is used in the validation;
- when a signature validation policy is not completely processed by the SVS, the report may provide information on constraints that have been ignored or overridden;
- when it is not possible to process the constraints submitted by the client, the report generated may provide information on the constraints that have been ignored or overridden;
- the signature validation report bears the identity of DigitalSign;
- the signature validation report shall report the signer's identity;
- it shall report all signed attributes. In case of a non-critical signed attribute, that cannot be decoded, it might be sufficient to just put information on the existence of the attribute;
- it contains a qualified timestamp;
- it can clearly indicate if the SVS did not perform the hash computation but relied on such a computation done by the user;
- it can clearly indicate the origin of each PoE (from within the signature, from the user, from the server);
- it contains the qualified electronic seal of DigitalSign;
- the signed validation reports are in the format and have the signature that may meet the requirements of ETSI TS 119 102-2;

- when presented via DigitalSign's website, validation takes place in a TLS session.

The report described in this section is considered proof of existence (PoE) of a signature.

3.5. QUALIFIED ELECTRONIC SIGNATURE VALIDATION

Requirements under Art. 32, 33 and 40 of Regulation (EU) No. 910/2014	Fulfilment by the service
Art. 32 Requirements for the validation of qualified electronic signatures	
1.The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that: a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;	The qualified electronic signature validation process fulfils the EU requirements for qualified trust service provider that issues qualified certificates for an electronic signature and for an electronic seal.
b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;	The qualified electronic signature validation process fulfils the EU requirements for qualified trust service provider that issues qualified certificates for an electronic signature and for an electronic seal.
c) the signature validation data corresponds to the data provided to the relying party;	This is guaranteed through the supported formats for electronic signature/seal.
d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;	The service automatically creates a validation report which contains the data from the electronic signature/seal certificates used for signing the document which the service has duly validated.
e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;	The pseudonym is written in a special attribute in the Subject field and this ensures that there is clear indication of this fact for the relying party.
f) the electronic signature was created by a qualified electronic signature creation device;	A special check whether the electronic signature was created by a qualified electronic signature creation device (SSCD for QSign/QSeal) takes place.

g) the integrity of the signed data has not been compromised;	This is ensured through the methodology for verification and validation of electronically signed documents described in this policy.
h) the requirements provided for in Article 26 were met at the time of signing.	The service verifies whether the advanced electronic signature placed meets the unique link to the signatory requirements, it identifies the signatory, it has been created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control and is linked to the data signed therewith in such a way that any subsequent change in the data is detectable. These checks are performed for all formats supported by the service.
2.The system used for validating the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.	This is ensured through the methodology for verification and validation of electronically signed documents described in this policy and practice.
Article 33 Qualified validation service for qualified electronic signatures	
1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who: a) provides validation in compliance with Article 32(1); and	The preceding paragraph describes how the Service fulfils the requirements of Art. 32.

b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.	This is ensured through the methodology for verification and validation of electronically signed documents and for the process of receiving the electronically signed report for validation described in this policy.
Article 40 Validation and preservation of qualified electronic seals	
Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.	The service also covers the validation of electronic seals within the meaning of Art. 40.