POLICY FOR PROVIDING OF QUALIFIED VALIDATION SERVICE OF QUALIFIED ELECTRONIC SIGNATURES AND QUALIFIED ELECTRONIC SEALS

PROVIDED BY

QUALIFIED TRUST SERVICE PROVIDER

INFONOTARY PLC

Version: 1.1

Entry into force 2.06.2023

TABLE OF CONTENTS

1. INTRODUCTION

The main purpose of this document POLICY FOR PROVISION OF QUALIFIED VALIDATION SERVICE OF QUALIFIED ELECTRONIC SIGNATURES AND QUALIFIED ELECTRONIC SEAL (Validation Policy) of the Qualified Trust Service Provider INFONOTARY PLC (Infonotary / Provider) is:

to describe and make public the rules, conditions and procedures that INFONOTARY has introduced and implements when providing the qualified service for validation of qualified certificates, qualified electronic signature and qualified electronic seal (Service / Validation Service);

to provide means for assessment of the compliance of the Provider's activity, including its reliability and security, with the provisions and requirements of Regulation (EU) 910/2014 and the relevant Bulgarian legislation.

to specify the main formats of the electronic signatures / seals to which the SERVICE is relevant;

to identify the components, protocols and interfaces of the Service and the links to other qualified services (eg CRL, OCSP, TSA) providing information to the validation service;

The policy is a public document and can be changed if necessary in case of changing regulatory, technological and procedural requirements, and any change in it is publicly available to all interested parties at: http://repository.infonotary.com and https://repository.infonotary.com.

1.1. COMPLIANCE

The Policy is prepared in accordance with the provisions and requirements of the following European and national regulations and standards:

- REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies pursuant to Articles 27(5) and 37(5) of 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
- Electronic Document And Electronic Trust Services Act;
- EN 319 401 v2.1.1 General Policy Requirements for Trust Service Providers;
- EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates
- 319 411-2 v2.1.1: Requirements for trust service providers issuing EU qualified certificates;
- EN 319 412 Certificate Profiles;

- ETSI TS 119 441 Policy Requirement for TSP providing signature validation services;
- ETSI TS 119 442: "Electronic Signatures and Infrastructures (ESI); Protocol for TSPs providing signature validation services";
- ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation";
- ETSI EN 319 102-1: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part1: Creation and Validation;
- ETSI TS 119 102-2: Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures, Part 2: Signature Validation Report;
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

1.2. GENERAL TERMS AND CONDITOIN

1.2.1. Trust Service Provider

INFONOTARY PLC is a Provider of Qualified Trust Services under Regulation (EU) No 910/2014 and has been granted qualified status by the Authority in accordance with the conditions laid down in Regulation (EU) No 910/2014 and in accordance with national law.

INFONOTARY PLC is a commercial company registered in the Commercial Register at the Registry Agency under UIC 131276827. The company has its registered office and address at 16, Ivan Vazov Str., Sofia, phone: +359 2 9210857, Internet address: http://www.infonotary.com. The company uses its registered trademark InfoNotary in its trade.

As a qualified provider INFONOTARY PLC performs the following activities and provides the following qualified certification services:

- Qualified certificate issuance and management services for Qualified electronic signature;
- Qualified certificate issuance and management services for Qualified electronic seal (including PSD2 certificates);
- Qualified certificate issuance and management services for Website authentication;
- Qualified certificate issuance and management services for Time stamps;
- Qualified validation service of qualified certificates, qualified electronic signature, and qualified electronic seal:
  - providing of services for on-line certificate status validation (OCSP) for Qualified certificates issued by InfoNotary;
  - providing of services for on-line validation of a qualified certificate, qualified electronic signature and qualified electronic seal (InfoNotary Qualified Validation Service).

In carrying out its activity INFONOTARY PLC applies the ISO/IEC 9001: 2008 certified Management System implemented in the company and ISO/IEC 27001: 2013 certified management system.

1.3. DENOMINATION AND IDENTIFICATION OF THE DOCUMENT

The **"Policy for provision of qualified validation service of the qualified electronic signatures and the qualified electronic seals"** document (Policy), is named **"InfoNotary CP QVS"** and is identified by the following Object identifier:

Policy name	Identifier (OID)
InfoNotary Qualified Validation Service	1.3.6.1.4.1.22144.3.5.2 0.4.0.19172.1

1.4. POLICY ADMINISTRATION

The certification policy and the Provider's practice are determined by the Board of Directors of INFONOTARY PLC.

Any and all amendments, modifications and additions to the qualified certification services provision practice and certification policies for the different qualified certificate types shall be adopted by the Board of Directors of INFONOTARY PLC.

The new versions of the documents shall be published in the Provider's Documentary repository immediately after their approval by the Board of Directors and shall be publicly accessible at: http://repository.infonotary.com and https://repository.infonotary.com.

Any and all comments, inquiries for information and clarifications of the qualified certification services provision practice and certification policies may be addressed to:

INFONOTARY PLC
1000 Sofia, Bulgaria
16 Ivan Vazov Str.
Tel:+359 2 9210857
e-mail: legal@infonotary.com
URL: www.infonotary.com

1.5. PARTICIPANTS IN THE VALIDATION SERVICE

The parties involved in the validation process are:

- Certification Authority and Operational Validation Certification Authority;
- Users/Relaying parties;
- External sources for the validation process:
  - Parties that have signed / sealed document (s);
  - Internal services of the Provider (certifying bodies - CA, TSA, CRL / OCSP);
  - National Trusted List;
  - European Trusted List.

1.6. CERTIFICATION AUTHORITY

InfoNotary is the Certification Authority of the Trust Service Provider carrying out the following activities: electronic signature and electronic seal certificates issuance, certificates management, including suspension, resumption and termination of certificates, keeping a register of certificates issued and providing access and means of constraint access to certificates.

The Certification Authority (root CA) controls Provider's Certification Policies defining the information types contained in the different types of End User Certificates, identifying the Holder/Creator information, application restrictions, and responsibilities.

The Certification Authority issues different types of certificates, according to the certification policies through its differentiated **Operational Certification Authorities** (operational CAs).

1.6.1. Operational Validation Certification Authority (InfoNotary Qualified Validated Service)

InfoNotary Qualified Validated Service Authority is an Operational Validation Authority that serves the process of validation of qualified certificates, qualified electronic signature, qualified electronic seal. Also issues and signs the qualified certificate supporting the advanced electronic seal, which signs the reports (results) of the performed validation checks of the certificates, signatures and seals.

The Certificate for the public key of the Operational Validation Authority **(InfoNotary Qualified Validation Services CA**), OID: 1.3.6.1.4.1.22144.3.5, is signed with the private key of the InfoNotary TSP Root, OID: 1.3 .6.1.4.1.22144.3.

The certificate of the **InfoNotary Qualified Validation Service** contains the following basic information:

InfoNotary Qualified Validation Services CA		
Basic x509 attributes:		
Attribute	**Value**	
Version		3 (0x02)
Serial number		Unique to the Provider's Register; 16-byte number
Start of validity period		Date and time of signing
End of validity period		Date and time of signing + 19 years
Algorithm of the electronic signature		SHA256/RSA
Attributes of the Issuer:		
Attribute		**Value**
Common Name	CN	InfoNotary TSP Root
Domain Component	DC	qualified-root-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		**Value**
Common Name	CN	InfoNotary Qualified Validation Services CA
Domain Component	DC	qualified-validation-ca
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827

Additional attributes of x509 extensions (x509v3 extensions):	
Attribute	**Value**
Basic Constraints (Critical)	Subject Type=CA
Key Usage (Critical)	Certificate Signing, CRL Signing
Public Key	RSA 3072 bits
Authority information Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/qualified-root-ca.crl
Certificate Policies (Non Critical)	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.5 [1.1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Validation Services CA
Subject Key Identifier	subjectKeyIdentifier
Authority Key Identifier	authorityKeyIdentifier=keyid,issuer

1.6.2. Relaying parties, Users / Subscribers

"Relaying Parties" are natural or legal persons who trust the certification services provided by Certification Service Providers. In the specific case of the Validation Service, the relying parties may be:

"User" and a natural or legal person using the Validation Service accessible through a web-based user interface at: https://www.infonotary.com/validate.

"Subscriber" is a natural or legal person who has a written contract with the Provider for the provision of the Validation Service, which is implemented as a web service for automatic validation.

The Relying parties should have the skills to use the Validation Service. They should acquaint and comply with all restrictions on the Service usage specified in this Policy, as well as to trust the results (reports) issued by the Provider.

1.6.3. Usage and accessibility of services

When practicable and depending on the certification service that is requested or provided to the Subscriber, as well as products related to its receipt, the Provider shall provide the opportunity for use by persons with disabilities. Accessibility to services and products is provided without prejudice to or exclusion of compliance with the requirements of security, relevance and compliance with the provisions of Regulation (EU) No 910/2014, the national legislation and internal policies and procedures of the Provider.

1.6.4. Limitations of the certification action activity

It is explicitly forbidden for third parties to use the validation services of INFONOTARY EAD in order to provide validation services to other third parties.

The Provider is not liable for damages resulting from the use of the validation service, beyond the permitted use and in accordance with the usage restrictions and will lead to cancellation of the guarantees that "INFONOTARY" EAD gives to users and relaying parties.

1.7. TERMS AND ABBREVIATIONS

Validation	Means the process of verifying and confirming that an electronic signature or a seal is valid
Qulified validation service	The validation service is provided by a qualified certification service provider, in accordance with Regulation 910/2014 (Articles 32, 33 and 40)
Validation data	Means data that is used to validate an electronic signature or an electronic seal.
Validation constrains	Technical criteria against which an electronic signature/seal can be validated
Validation report	Report from the signature / seal validation process, which is presented to the user
Status indicators	One of the following status indicators contained in the report - VALID (TOTAL-PASSED), INVALID (TOTAL-FAILLED) or UNDEFINED (INDETERMINATE).
Electronic seal	Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
Qualified electronic time stamp	Qualified electronic time stamp shall meet the following requirements: (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; (b) it is based on an accurate time source linked to Coordinated Universal Time; and (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method

Qualified electronic seal	An advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal
Qualified electronic signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures
Qualified certificate for electronic seal	A certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III, Regulation EU 910/2014
Qualified certificate for electronic signature	A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I, Regulation EU 910/2014
Qualified trust service	A trust service that meets the applicable requirements in Regulation EU 910/2014
Practice	Certification Practice Statement is a document containing rules on the issuance, suspension, renewal and revocation of certificates, the conditions for certificates access InfoNotary Qualified CPS
Policy	Policy For Provision Of Qualified Validation Service Of The Qualified Electronic Signatures And The Qualified Electronic Seals
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
Regulation GDPR	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)

ABBREVIATIONS

ASN.1	Abstract Syntax Notation One – Abstract object-description language for certificates
CA	Certification Authority
CC	Common Criteria
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CP	Certificate Policy
CPS	Certification Practice Statement
CRC	Communications Regulation Commission
CRL	Certificate Revocation List - List of suspended and revoked certificates
DN	Distinguished Name - Unique name
ETSI	European Telecommunications Standards Institute
EU	European Union
EBA	European Banking Authority
FIPS	Federal Information Processing Standard
IEC	International Electrotechnical Commission
ISO	International Standardization Organization
LDAP	Lightweight Directory Access Protocol - A protocol for simplified directory access
NCA	National Competent Authority
OID	Object Identifier
OCSP	On-line Certificate Status Protocol – Protocol for real-time checking of certificate status
PKCS	Public Key Cryptography Standards – Cryptographic standard for public key transfer

PKI	Public Key Infrastructure
PSD2	Payment Service Directive 2
PSP	Payment Service Provider
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider issuing Card-based payment instruments
PSP_AI	Payment Initiation Service Provider
RA	Registration Authority
RSA	Rivest-Shamir-Adelman – Cryptographic algorithm for signature generation
SSCD	Secure Signature Creation Device
RQSCD	Remote Qualified Electronic Signature Creation Device
QSCD	Qualified Signature Creation Device
SHA	Secure Hash Algorithm – Hash Algorithm for hash identifier extraction
SSL	Secure Socket Layer – Secure data transmission channel
URL	Uniform Resource Locator

1.8. USE OF VALIDATION CERTIFICATES

The validation service uses the following service certificates:

- Root Certificate, Operational Validation Certification Authority (InfoNotary Qualified Validation Services CA);
- Qualified certificate supporting advanced electronic seal;
- Certificate of website authentication.

The **InfoNotary Qualified Validation Services** CA's certificate is used to sign the Qualified certificate supported advanced electronic seal.

The reports (results) of the performed validation sessions are sign with he qualified certificate supported advanced electronic seal.

The certificate of website authentication performs online authentication of the validation service before the User and provides a secure communication channel / secure session with the User during usage the service.

Qualified certificate supporting advanced electronic seal, has the following profile:

InfoNotary Qualified Validation Stamp		
Basic x509 attributes:		
Attribute		**Value**
Version		3 (0x02)
Serial number		Unique for the Provider's register; 16-byte number
Valid from		Date and time of signing
Valid to		Date and time of signing + 5 years
Signature Algorithm		SHA256/RSA
Issuer:		
Attribute		**Value**
Domain Component	DC	qualified-validation-ca
Common Name	CN	InfoNotary Qualified Validation Services
Country Name	C	BG
Locality Name	L	Sofia

Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	Qualified TSP
Organization Identifier	2.5.4.97	NTRBG-131276827
Attributes of the Holder (x509 Subject DN):		
Attribute		**Value**
Domain Component	DC	qualified-validation-ca
Common Name	CN	InfoNotary Qualified Validation Stamp
Country Name	C	BG
Locality Name	L	Sofia
Organization Name	O	InfoNotary PLC
Organizational Unit Name	OU	InfoNotary Qualified Validation Services
Organization Identifier	2.5.4.97	NTRBG-131276827

Additional attributes of x509 extensions (x509v3 extensions):	
Attribute	**Value**
Basic Constraints (Critical)	End entity
Key Usage (Critical)	Digital Signature, Non-Repudiation
Public Key	RSA 2048 bits
Authority Key Identifier	AuthorityKeyIdentifier
Subject Key Identifier	SubjectKeyIdentifier
Authority information Access	[1] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= https://repository.infonotary.com/qualified-validation-ca.crt [2] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)

	Alternative Name: URL= http://ocsp.infonotary.com/qualified
CRL Distribution Point (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.infonotary.com/crl/ qualified-validation-ca.crl
	[1]Certificate Policy: Policy dentifier=0.4.0.194112.1.1 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.22144.3.5.2 [2.1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://repository.infonotary.com/cps/qualified-tsp.html Unotice: InfoNotary Qualified Validation Service [3] Certificate Policy: Policy dentifier=0.4.0.19172.1
Qualified Certificate Statement (Non Critical)	id-etsi-qcs-semanticsld-Legal (oid=0.4.0.194121.1.2) id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1) id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2) (oid=0.4.0.1862.1.2) id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5) PDSLocation=https://repository.infonotary.com/pds/pds_bg.pdf Language=bg PDSLocation=https://repository.infonotary.com/pds/pds_en.pdf Language=en
Extended Key Usage (Non Critical)	

2 SERVICE VALIDATION DESCRIPTION

The INFONOTARY's validation qualified service allows to confirm the validity of a qualified certificate, a qualified electronic signature and a qualified electronic seal, in case that:

- The certificate for the creation of the signature / seal at the time of signing / sealing is qualified in accordance with Annex I to the Regulation 910/2014.
- The qualified certificate was issued by a qualified trust service provider and was valid at the time of signing
- the signature validation data corresponds to the data provided to the relying party;
- the unique set of data representing the signatory in the certificate is correctly provided to 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 signature/seal was created by a qualified electronic signature/seal creation device;
- the integrity of the signed data has not been compromised;
- At the time of signing the requirements for advanced electronic signature are met (Article 26 of the Regulation).

The qualified validation service of INFONOTARY provides an opportunity for the Users and the Relaying parties to receive the result of the validation process (report) in an automated way with a status indicator that is reliable and accurate and is sealed with a Provider's qualified certificate supporting advanced electronic seal.

The Provider's qualified validation service verifies only the technical validity of the qualified certificate, the qualified signature and the seal.

The technical validity of the qualified certificate, qualified signature and seal is checked in accordance with the process described in ETSI TS 319 102 and ETSI TS 119 172-4 and confirmed by signing the result (report) with the Provider's qualified certificate supporting advanced electronic seal.

The Qualified Validation Service allows to verify the following signature formats and profiles:

Formats/Profiles	**BASELINE_B**	**BASELINE_T**	**BASELINE_LT**	**BASELINE_LTA**
CAdES	√	√	√	√
XAdES	√	√	√	√
PAdES	√	√	√	√
ASiCS/ ASiCE	√	√	√	√

JadES	√	√	√	√

All certificates and related certification chains are validated against the European Trust List (EU TSL- https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home).

2.1. VALIDATION SERVICE COMPONENTS

The qualified InfoNotary Qualified Validation Service (IQVS) includes the following software components, according to ETSI TS 319 102:

- Application for signature/seal validation - software agent by the User site. It can be a software or web client that runs through a browser and has the following functionality:
  - Creates validation requests;
  - Executes the validation protocol by the user site;
  - Presents the validation report.
- Validation server - performs the following functionalities on the Provider's site:
  - Receives electronic signatures/seals and other input data from the client for validation;
  - Performs the validation process in accordance with the applicable Policy and constraints, using processes, algorithms and validation protocols according to ETSI EN 319 102-1 and ETSI TS 119 442;
  - Communicates with internal and external sources of the service - CRL/OCSP, Certification Authority, TSA, EU Trusted List;
  - Generates a report and status indicator of the validated signature / seal.

2.2. INTERFACE AND VALIDATION SERVICE PROVISION

The validation service is available at - https://www.infonotary.com/validate. INFONOTARY provides the qualified validation service through following interfaces:

- Web-based user interface (Signature Validation Application - SVA), which uses a secure communication channel/secure session (HTTPS protocol / certificate of website authentication) to connect to the validation server. After accessing the service, the User (the Relying Party) uploads an electronically signed / sealed file or certificate that he wishes to verify, selects the parameters of the request and sends the request to the validation server.
- Web service - provided through an application programming interface for automatic validation, and the terms for provision are settled in a contract between the Provider and the Relying Party.

2.3. VALIDATION PROCESS

The validation process goes through the following steps according to ETSI TS 319 172-1:

Electronic signature/seal validation requests and the responses to these requests use client-server communication. The validation protocol is in accordance with ETSI EN 119 442.

Step 1: The SVA / web client generates and sends a validation request that contains the signed / sealed document or sends a document and signature;

Step 2: The validation server validates the electronic signature / seal using the Provider's internal services (CRL, OCSP, TSA) or external services of other providers or external sources of certificates (European Trusted List).

Step 3: The validation server generates and sends a validation report. The report is sealed with an advanced seal supported by qualified certificate of Infonotary.

Step 4: The web client visualizes the validation report in pdf format and it can be saved, locally on the user's computer, or printed.

The validation service supports the following processes of validation of the qualified electronic signatures and seals in different formats:

- validation process of the signature /seal with basic format/profile BASELINE;
- Time stamp validation process;
- validation process of the signature/seal with BASELINE_T and BASELINE_LT profile;
- validation process of the signature/seal with BASELINE_LTA profile.

For each qualified electronic signature/seal format, the validation service performs the following actions sequentially:

- Performs the validation process of the electronic signature/seal with extended format - BASELINE_T, BASELINE_LT and BASELINE_LTA;
- Performs the validation process of the electronic signature/seal with basic format – BASELINE;
- If the validation status of the selected validation process is PASSED, a TOTAL-PASSED status indicator and a validation report are returned;
- If the validation status of the selected validation process is FAILED, a TOTAL-FAILED status indicator and a validation report are returned;
- If the validation status of the selected validation process is neither VALID nor FAILED, the UNDEFINED status indicator and validation report are returned.

2.4. STATUS INDICATORS AND VALIDATION REPORT

2.4.1. Status indicators

The validation status of the qualified signature / seal can be:

Reported Validation Information		Semantics
Status-indication	**Associated Validation report data**	
TOTAL- PASSED	The validation process shall output the validated certificate chain, including the signing certificate, used in the validation process. In addition, the validation process may provide the result of the validation for each of the validation constraints. The validation process should provide the DA access to the signed attributes present in the signature, the identity of the signer.	The signature validation process results into TOTAL-PASSED based on the following considerations: • the format check succeeded; • the cryptographic checks of the signature succeeded (including checks of hashes of individual data objects that have been signed indirectly); • any constraints applicable to the signer's certificate have been positively validated (e.g. the signing certificate consequently has been found trustworthy); and • the signature has been positively validated against the validation constraints and hence is considered conformant to these constraints.
TOTAL-FAILED	The validation process shall output 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 signature validation process results into TOTAL-FAILED because the format-check failed, cryptographic checks of the signature failed (including checks of hashes of individual data objects that have been signed indirectly) or it has been proven that the signing certificate was invalid at the time of generation of the signature
INDETERMINATE	The validation process shall output additional information to explain the INDETERMINATE indication and to help the verifier to identify where relevant what data is missing to complete the validation process. In particular, it shall provide validation result indications for those validation constraints that have been taken into account and for which an indeterminate result occurred.	The available information is insufficient to ascertain the signature to be *TOTAL-PASSED* or *TOTAL-FAILED*.

When the validation status is TOTAL-FAILED and INDETERMINATE, the validation report also contains additional indicators as follows:

Reported Validation Information			Semantics
Main status indication	**Sub-indication Associated Validation report data**	**Sub-indication Associated Validation report data**	
TOTAL-FAILED	FORMAT_FAILURE	The validation process shall provide any information available why parsing of the signature failed.	The signature is not conformant to one of the base standards to the extent that the cryptographic verification building block is unable to process it.

	HASH_FAILURE	The validation process shall provide: An identifier (s) (e.g. an URI or OID) uniquely identifying the element within the signed data object (such as the signature attributes, or the SD) that caused the failure.	The signature validation process results into TOTAL-FAILED because at least one hash of a signed data object(s) that has been included in the signing process does not match the corresponding hash value in the signature.
	SIG-CRYPTO-FAILURE	The validation process shall output: The signing certificate used in the validation process.	The signature validation process results into TOTAL-FAILED because the signature value in the signature could not be verified using the signer's public key in the signing certificate.
	REVOKED	The validation process shall provide the following: - The certificate chain used in the validation process. - The time and, if available, the reason of revocation of the signing certificate.	The signature validation process results into *TOTAL-FAILED* because: • the signing certificate has been revoked; and • there is proof that the signature has been created 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.
INDETERMINATE	*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.
	SIG_CONSTRAINTS_FAILURE	The validation process shall provide: The set of constraints that have not been met by the signature.	The signature validation process results into *INDETERMINATE* because one or more attributes of the signature do not match the validation constraints
	CHAIN_CONSTRAINTS_FAILURE	The validation process shall output: • The certificate chain used in the validation process. • The set of constraints that have not been met by thechain.	The signature validation process results into *INDETERMINATE* because the certificate chain used in the validation process does not match the validation constraints related to the certificate
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The process shall output: Additional information regarding the reason.	The signature validation process results into *INDETERMINATE* because the set of certificates available for chain validation produced an error for an unspecified reason.
	CRYPTO_CONSTRAINTS_FAILURE	The process shall output: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below	The signature validation process results into *INDETERMINATE* because at least one of the algorithms that have been used in material (e.g. the signature value, a certificate...) involved in

		the required cryptographic security level. • If known, the time up to which the algorithm or key size were considered secure.	validating the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and: • this material was produced after the time up to which this algorithm/key was considered secure (if such a time is known); and • the material is not protected by a sufficiently strong time-stamp applied before the time up to which the algorithm/key was considered secure (if such a time is known).
	POLICY_PROCESSIN G_ ERROR	The validation process shall provide additional information on the problem.	The signature validation process results into *INDETERMINATE* because a given formal policy file could not be processed for any reason (e.g. not accessible, not parseable, digest mismatch, etc.).
	SIGNATURE_POLICY _NOT_AVAILABLE	-	The signature validation process results into *INDETERMINATE* because the electronic document containing the details of the policy is not available
	TIMESTAMP_ORDER_ FAILURE	The validation process shall output the list of time-stamps that do no respect the ordering constraints.	The signature validation process results into *INDETERMINATE* because some constraints on the order of signature time-stamps and/or signed data object(s) time-stamps are not respected
	NO_SIGNING_CERTI FICATE_FOUND	-	The signature validation process results into *INDETERMINATE* because the signing certificate cannot be identified.
	NO_CERTIFICATE_C HAI N_FOUND	-	The signature validation process results into *INDETERMINATE* because no certificate chain has been found for the identified signing certificate
	REVOKED_NO_POE		The signature validation process results into INDETERMINATE because the signing certificate was revoked at the validation date/time. However, the Signature Validation Algorithm cannot ascertain that the signing time lies before or after the revocation time.
	REVOKED_CA_NO_P OE	The validation process shall provide the following: • The certificate chain which includes the revoked CA certificate. • The time and the reason of revocation of the certificate.	The signature validation process results into INDETERMINATE because at least one certificate chain was found but an intermediate CA certificate 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 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.
	CRYPTO_CONSTRAINTS_FAILURE_NO_POE	The process shall output: • Identification of the material (signature, certificate) that is produced using an algorithm or key size below the required cryptographic security level. If known, the time up to which the algorithm or key size were consider secure.	The signature validation process results into *INDETERMINATE* because at least one of the algorithms that have been used in objects (e.g. the signature value, a certificate, etc.) involved invalidating the signature, or the size of a key used with such an algorithm, is below the required cryptographic security level, and there is no proof that this material was produced before the time up to which this algorithm/key was considered secure
	NO_POE	The validation process shall identify at least the signed objects for which the POEs are missing. The validation process should provide additional information on the problem.	The signature validation process results into *INDETERMINATE* because a proof of existence is missing to ascertain that a signed object has been produced before some compromising event (e.g. broken algorithm).
	TRY_LATER	The validation process shall output the point of time, where the necessary revocation information is expected to become available.	The signature validation process results into *INDETERMINATE* because not all constraints can be fulfilled using available information. However, it may be possible to do so using additional revocation information that will be available at a later point of time.
	SIGNED_DATA_NOT_FOUND	The process should output when available: The identifier(s) (e.g. an URI) of the signed data that caused the failure.	The signature validation process results into *INDETERMINATE* because signed data cannot be obtained.

	GENERIC	The validation process shall output: Additional information why the validation status has been declared INDETERMINATE.	The signature validation process results into INDETERMINATE because of any other reason.

2.4.2 Validation report

The results of the validation process are presented in a basic and detailed report, as well as in machine-readable XML format, in accordance with ETSI TS 119 102-1.

The basic report contains:

- Validation Policy;
- Status-indicators;
- Date and time (GMT) of creation of the signature / seal;
- The format/ profile of the validated signature / seal;
- Name of the Holder / Creator of the signature / seal;
- Information about the signed / sealed document (name, number of signatures).

The validation status-indicators that SVA provides after validation of the specific format/ profile of the signature / seal according to the Validation Policy is:

- TOTAL-PASSED - the checks of all cryptographic characteristics / parameters of the signature / seal are successful, as well as those in accordance with the Validation Policy;
- TOTAL-FAILED - the checks of all cryptographic characteristics / parameters of the signature / seal are unsuccessful, or the signature / seal is created after cancellation / termination of the qualified certificate or the format does not correspond to some basic formats;
- INDETERMINATE - the results of the individual / single checks do not allow the signature / seal to be assessed as TOTAL-PASSED or TOTAL-FAILED.

The detailed report includes complete information for checks of all limitations, possible values and additional reporting data related to these values, according to the Validation Policy.

3 Validation constrains

The validation process is controlled by a set of validation constraints. These restrictions are set when managing the service and can be defined in the following general groups:

- X.509 validation constraints;
- cryptographic constraints of the signature / seal;
- constraints on the elements of the signature / seal.

3.1. COMMON CONSTRAINS

The validation status indicator contained in the report only shows whether a signature / seal is technically valid under this Validation Policy. The maximum size of a signed / sealed data file to be checked is 10 MB (megabytes).

3.2. X.509 CONSTRAINS

The validation service fulfills the following constrains when validating X.509 certificates (ETSI TS 119 172-1 [4], point A.4.2.1, table A.2 row m).

Constraint(s)	Constraint value at signature validation
m)1. X509CertificateValidationConstraints: This set of constraints indicates requirements for use in the certificate path validation process as defined in IETF RFC 5280. These constraints may be different for different certificate types (e.g. certificates issued to signer, to CAs, to OCSP responders, to CRL Issuers, to Time-Stamping Units). 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.	EU Trusted List
(m)1.2. CertificationPath: This constraint indicates a certification path required to be used by the SVA for validation of the signature. The certificate path is of length 'n' from the trust anchor (TA) down to the certificate used in validating a signed object (e.g. the signer's certificate or a time stamping certificate). This constraint can include the path to be considered or indicate the need for considering the path provided in the signature if any. (m)1.3. user-initial-policy-set: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (c) (m)1.4. initial-policy-mapping-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (e) (m)1.5. initial-explicit-policy: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (f) (m)1.6. initial-any-policy-inhibit: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (g) (m)1.7. initial-permitted-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (h) (m)1.8. initial-excluded-subtrees: This constraint is as described in IETF RFC 5280 clause 6.1.1 item (i) (m)1.9. path-length-constraints: This constraint indicates restrictions on the number of CA certificates in a certification path. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it) (m)1.10. policy-constraints: This constraint indicates requirements for certificate policies referenced in the certificates. This may need to define initial values for this or to handle such constraint differently (e.g. ignore it). This should also allow the ability to require a (possible set of) specific certificate policy extension value(s) in end-entity certificates (without requiring such values appearing in certificate of authorities in the certification path).	None
(m)2. RevocationConstraints: This set of constraints indicates requirements applicable when verifying the certificate validity status of the certificates during the certificate path validation process. These constraints may be different for different certificate types (e.g. certificates issued to signer, to	eitherCheck

CAs, to OCSP responders, to CRL Issuers, to Time- Stamping Units). Semantic for a possible set of requirement values used to express such requirements is defined as follows: (m)2.1. RevocationCheckingConstraints: This constraint indicates requirements for checking certificate revocation. Such constraints may specify if revocation checking is required or not and if OCSP responses or CRLs have to be used. Semantic for a possible set of requirement values used to express such requirements is defined as follows: clrCheck: Checks shall be made against current CRLs (or Authority Revocation Lists); ocspCheck: The revocation status shall be checked using OCSP IETF RFC 6960; bothCheck: Both OCSP and CRL checks shall be carried out; eitherCheck: Either OCSP or CRL checks shall be carried out; noCheck: No check is mandated	
(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 and the time of validation or require the SVA to only accept revocation information issued a certain time after the signature has been created.	None
(m)2.3. RevocationInfoOnExpiredCerts: This constraint mandates the signer's certificate used in validating the signature to be issued by a certification authority that keeps revocation notices for revoked certificates even after they have expired for a period exceeding a given lower bound.	None
(m)3. LoAOnTSPPractices: This constraint indicates the required LoA on the practices implemented by the TSP(s) having issued the certificates to be validated during the certificate path validation process, i.e. the certificates present in the certificate path of the signer's certificate, and optionally those present in all or some of the other certificate chain	None
EUQualifiedCertificateRequired	Yes
EUQualifiedCertificateSigRequired	Yes
EUQualifiedCertificateSealRequired	Yes

3.3. CRYPTOGRAPHIC CONSTRAINTS

The cryptographic constrains of the validation service regarding the cryptographic algorithms and parameters used in the creation of signatures / seals or used in the validation of signed objects (ETSI TS 119 172-1 [4], point A.4.2.1, table A.2 row) are:

Constraint(s)	**Constraint value at signature validation**
(p)1. CryptographicSuitesConstraints: This constraint indicates requirements on algorithms and parameters used when creating signatures or used when validating signed objects included in the validation or augmenting process (e.g. signature, certificates, CRLs, OCSP responses, time-stamps).	Based on ETSI TS 119 312 [ETSI 119 312]

3.4. CONSTRAINTS ON THE ELEMENTS OF THE SIGNATURE / SEAL

The validation service supports any additional constrains to the above X.509 certificates and cryptographic constrains of the signature / seal elements as specified in ETSI TS 119 172-1 [ETSI 119 172-1], point A.4.2.1, table A.2 row b.

Constraint(s)	Constraint value at signature validation
(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 indicate the required content related information elements under the form of signed or unsigned qualifying properties that are mandated to be present in the signature. This 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 sig	None
(b)3. DOTBSAsAWholeOrInParts: This constraint indicates whether the whole data or only certain part(s) of it have to be signed. 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

4 COMPLIANCE WITH REGULATION 910/2014 (Art. 32 and 33)

Requirements under Art. 32 of the Regulation (EU) No. 910/2014	Performance by the SERVICE
the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I	The certificates validation process complies with the requirements described in EU Decision 2015/1505 and ETSI 319 412
the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing	The certificates validation process complies with the requirements described in EU Decision 2015/1505 and ETSI 319 412
the signature validation data corresponds to the data provided to the relying party	The validation process provides the Users / Relying Party with a report including the Certificate of the Holder / Creator, containing the validation data (public key, etc.). See the Validation Report in the DSS User's Guide
the unique set of data representing the signatory in the certificate is correctly provided to the relying party	The validation process provides the Users / Relying Party with a report including the Certificate of the Holder / Creator, containing the validation data (public key, etc.). See the Validation Report in the DSS User's Guide
the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing	The validation process provides the Users / Relying Party with a report including the Certificate of the Holder / Creator, containing the validation data (public key, etc.). See the Validation Report in the DSS User's Guide
the electronic signature was created by a qualified electronic signature creation device;	The certificates validation process complies with the requirements described in EU 2015/1505 for QTSP issuing qualified certificates. A check for the required type of SSCD (QSCD) is performed.
the integrity of the signed data has not been compromised	It is guaranteed through the supported validation model indicated in this document. See "Cryptographic constrains" ETSI TS 119-312
the requirements provided for in Article 26 were met at the time of signing	The signature /seal validation process verifies the status and attributes of the certificate at the time the signature is generated
Requirements under Art. 33 of the Regulation (EU) No. 910/2014	**Performance by the SERVICE**
A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider	Infonotary is the QTSP in accordance with Regulation 910/2014 and the national Electronic Signature and Electronic Certification Services Act

5 EQUIPMENT, PROCEDURE AND MANAGEMENT CONTROL

According to item 5 of the document of INFONOTARY "CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES".

6 TECHNICAL SECURITY CONTROL

According to item 6 of the document of INFONOTARY "CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES".

7 AUDITING AND CONTROL OF THE ACTIVITY

According to item 8 of the document of INFONOTARY "CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES".

8 OTHER BUSINESS AND LEGAL CONDITIONS

According to item 9 of the document of INFONOTARY "CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED CERTIFICATION SERVICES".