ISO 9001:2015 ISO 27001:2013
ISO 20000-1:2018 ISO 22301:2019
Regulation (EU) 910/2014
Regulation (EU) 2016/679

POLICY AND PRACTICE

FOR QUALIFIED VALIDATION SERVICE OF QUALIFIED

ELECTRONIC SIGNATURES/SEALS

CONTENTS

1. INTRODUCTION

This document defines the rules for qualified validation of electronic signatures and seals and for issuance of electronically signed reports through the trust service for qualified validation "Evrotrust Qualified Validation Service". Electronically signed reports constitute electronic documents generated automatically, which contain the result of the validation of the electronic signature/seal. These reports are electronically signed by the validating authority of Evrotrust.

This document has been developed by "Evrotrust Technologies" AD (Evrotrust) in accordance with the requirements laid down in Regulation (EU) No. 910/2014[1] and in accordance with ETSI TS 119 441.

1.1. OVERVIEW

Digital signatures are a major cornerstone for electronic transactions, provided they can be validated in such a way that users and relying parties have full confidence in the fact that they answer their (business) needs. In this perspective, the user and the relying party may address Evrotrust, which, in its capacity as a qualified signature validation service provider (QSVSP), will perform the validation of the digital signature on their behalf. The outcome of this procedure is a signature validation report. Participants of electronic transactions need to have confidence that Evrotrust has properly established procedures and protective measures in order to minimise the operational and financial threats and risks associated with digital signatures.

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

[1] *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*

Evrotrust provides the service in accordance with the requirements laid down in Regulation (EU) No. 910/2014 and guarantees that this service:

- Applies operational procedures and security management procedures that exclude any possibility for manipulation of the data and the status of the validated certificates; or
- Checks the validity of the electronic signature/seal in line with the requirements of Article 33 of Regulation (EU) No. 910/2014;
- Checks the status of the certificates in accordance with Recommendation RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- Validates qualified certificates and electronic signatures/seals;
- Fulfils the technical procedures for validation of signatures in line with the requirements of ETSI TS 319 102-1 and ETSI TS 119 172-4;
- Evrotrust (QSVSP) can provide additional information about the signature or the seal, e.g. if it is an advanced electronic signature/seal based on a qualified certificate;
- In order to guarantee the proper functioning of the validation service, Evrotrust tests each change in the validation service functionality and the tests are saved in the internal documentation of Evrotrust. The tests are subject to verification and statements;
- The validation report bears the electronic seal of Evrotrust;
- 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;
- Evrotrust 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.

1.1.1. PROVIDER IDENTIFICATION

The service provider is Evrotrust Technologies AD and is identified with a registered object identifier (OID):1.3.6.1.4.1.47272.

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

1.1.2. SUPPORTED POLICIES

Evrotrust assigns an object identifier (OID) to each policy, based on which the qualified certificates issued by Evrotrust are validated.

The object identifier value for a policy followed by Evrotrust is as follows:

Validating authority (QESValidation/Q)	**Object Identifier (OID)**
Evrotrust Qualified Validation Service Policy of the validating authority for the needs of the electronic signature and seal certificates under Regulation (EU) No. 910/2014	1.3.6.1.4.1.47272.2.9

It corresponds to ETSI TS 119 441 specific OID: itu-t(0) identified-organization(4) etsi(0) val-service-policies(19441) policy-identifiers(1) qualified (2).

Evrotrust identifies the service policies supported in accordance with ETSI EN 319 401. The validation service of Evrotrust enters the applicable OID of the policy used in the responses, reports and documents provided to the users and the relying parties.

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

1.1.3. 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".

1.2. SIGNATURE VALIDATION SERVICE COMPONENTS

1.2.1. SIGNATURE VALIDATION SERVICE (SVS) ACTORS

The two main actors are Evrotrust (QSVSP) which is a qualified trust service provider (QTSP) and its subscriber. The QSVSP may offer one or more signature validation services based on contractual relations. The electronic signature/seal validation service may be combined with a service for enhancing the signature reliability in accordance with the protocol indicated in ETSI TS 119 442 which supports the order for enhancing the reliability of the signature with the validation service.

The subscriber may be an application or a human being (user) interacting with the application for signature validation.

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

- The signer - the signer can set constraints on the signature (e.g. by means of a signature creation policy) and this may influence the signature validation;
- The signers' related trust service providers (TSP):
  - The TSP having issued the signer's certificate (CA);
  - Any TSP that can be implied in the signature generation:
- Other TSPs (TSAs; QSVSP, etc.)
- The European or foreign trusted list providers;
- The European Commission providing the trusted list of qualified service providers.

1.2.2. VALIDATING AUTHORITY

"Evrotrust Qualified Validation Service" is a validating authority that services electronic signature and seal certificates under Regulation (EU) No. 910/2014. Evrotrust's Validating Authority signs the validation reports issued for the validated electronically signed documents electronically with a qualified electronic seal certificate.

The qualified certificate for electronic seal of **„Evrotrust Qualified Validation Service"** is:

Version	V3	
Serial number	38 00 00 00 05 f0 08 5a 0a b9 a3 69 64 00 00 00 00 00 00 05	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	14 February 2018 12:16:20 UTC	
Valid to	14 February 2023 12:26:20 UTC	

Subject	CN=	Evrotrust Qualified Validation Service
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Subject Key Identifier	5d 19 73 73 35 60 65 a1 62 e7 c2 0d d1 fe 63 e5 4f 90 c8 1a	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.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://ca.evrotrust.com/ocsp	
Key Usage (critical)	Digital Signature, Non-Repudiation (c0)	

Basic Constrains (critical)	Subject Type=End Entity Path Length Constraint=None

The qualified certificate for electronic seal of **„Evrotrust Qualified Validation Service SU"** is:

Version	V3	
Serial number	72 dc e5 b1 c8 ec e7 58 39 6f 7f 2e 1b e8 06 15 6e 7e b2 1b	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Valid from	13 July 2019, 15:45:22 UTC	
Validit to	11 July 2024, 15:45:22 UTC	
Subject	CN=	Evrotrust Qualified Validation Service SU
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Authority Key Identifier	KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.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://services.evrotrust.com/ocsp	

<table>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.9
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)</td></tr>
<tr><td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)</td></tr>
<tr><td>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)</td><td>PdsLocations:
PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
language=en</td></tr>
</table>
</td></tr>
<tr><td>CRL Distribution Points</td><td>[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://services.evrotrust.com/EvrotrustServicesCA.crl</td></tr>
<tr><td>Subject Key Identifier</td><td>c5 da 13 76 8c ad fd fa 9e e3 2b 80 99 42 6e c7 3a f7 3c 1c</td></tr>
<tr><td>Basic Constrains (critical)</td><td>Subject Type=End Entity
Path Length Constraint=None</td></tr>
<tr><td>Key Usage (critical)</td><td>Digital Signature, Non-Repudiation (c0)</td></tr>
</table>

Thumbprint (SHA1): 9372295a5d83b7bd27dda84a9fb88f164363ca60

Thumbprint (SHA256):

c43e0882978f98ceca29360083ab1ea5a277740714e9c6dbcc023b1618d3549a

Filename: "Evrotrust Qualified Validation Service SU.pem.cer"

1.2.3. SERVICE ARCHITECTURE

The validation service consists of the following components:

- The signature validation client is a component or a piece of software that implements the signature validation protocol on the user's side. In particular it:
  - Requests a signature validation to the signature validation service server (SVSServ);
  - It is possible to request the validation of multiple signatures in accordance with ETSI TS 119 442;
  - Executes the signature validation protocol (SVP) on the user's side;
  - When applicable, takes care of the validation report presentation;

The client can incorporate:

- A user interface for manual input of the request; or
- A machine interface for automated requests;
- A user interface to present the report. The applicability checking, i.e. the final decision to "accept" a signature on the basis of the validation report can be done by the user (manually), or by the client or the server (depending on the SVS implementation). This can be done according to signatures applicability rules that are specified in ETSI TS 119 172-1;

- The signature validation service server (SVSServ) which is the component of the service that implements the signature validation protocol on the QSVSP's side. In particular it:
  - Executes the signature validation service protocol and processes the signature validation;
  - Runs the signature validation application (SVA) such as defined in ETSI TS 119 102-1, which includes implementation of the validation algorithm defined in ETSI TS 119 102-1. For this purpose, Evrotrust allows for the service to call external factors, such as the CA having issued

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

- Creates the signature validation report(s);
- Builds the signature validation response. SVSServ implements the SVA as laid down in ETSI TS 119 102-1. In certain cases the Driving Application (DA) can be fully on the client side or shared over client and server (the signature validation service server can implement part of the DA, e.g. to perform some applicability check). The present document does not put requirements on the client. Only the DA's elements implemented on the server side are subject to requirements.

1.3. DEFINITIONS AND ABBREVIATIONS

1.3.1. DEFINITIONS

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

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

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

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

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

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

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

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

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

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

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

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

signature validation application (SVA) - an application that validates a signature against a signature validation policy, and that outputs an indication of the signature validation status and a signature validation report. The signature validation application is specified in ETSI TS 119 102-1;

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

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

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

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

Signature Validation Service (SVS) policy – this is a set of rules that indicate the quality and the applicability of a signature validation service. The document determines the service applicability to a particular community and/or class of application with common security requirements. The SVS policy is applicable to a trust service as defined in ETSI EN 319 401;

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

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

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

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

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

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

signature validation constraint - technical criteria against which a digital signature can be validated, as specified in ETSI TS 119 102-1;

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

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

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

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

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

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

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

1.3.2. ABBREVIATIONS

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

DA - Driving Application;

OVR – OveRall/General requirements applicable to more than 1 (one) component;

PoE - Proof of Existence;

QES - Qualified Electronic Signature or Qualified Electronic Seal;

(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;

SVS - Signature Validation Service;

QSVSP - Qualified Signature Validation Service Provider;

SVSServ - Signature Validation Service Server;

TSA - Time Stamping Authority;

VPR - signature Validation Process.

1.4. POLICY, PRACTICE STATEMENT AND GENERAL TERMS REQUIREMENTS

1.4.1. ORGANISATION MANAGING THE DOCUMENTATION OF EVROTRUST

Evrotrust is responsible for the management of the public documentation, including this document. Each new version of any document shall be effective until the moment of approval and publication of a new version. Each new version shall be developed by Evrotrust employees and shall be published after approval of the Board of Directors of Evrotrust.

Users shall only take into account the effective version of the Practices and Policies as of the time of using the services of Evrotrust.

This document is inextricably linked to the document "Qualified Trust Service Practice Statement".

1.4.2. CONTACT PERSON

The contact person for management of the document "Qualified Validation Policy and Practice Statement" of Evrotrust Technologies AD shall be the Chief Executive Officer of Evrotrust.

Further information can be requested at the following address:

Evrotrust Technologies AD

Sofia, 1766

Business center MM, floor 5, "Okolovrasten pat" 251G

telephone, Fax: + 359 2 448 58 58

email: office@evrotrust.com

1.4.3. APPLICABILITY OF EVROTRUST'S PUBLIC DOCUMENTATION

Evrotrust's public documentation which is related to the provision of the qualified validation service has been made available to all stakeholders and is published on the internet on Evrotrust's website: https://www.evrotrust.com/landing/en/a/tsp-documents. The set of documents related to the qualified validation service includes:

- "Policy aNd Practice for qualified validation service of qualified electronic signatures/seals" with OID: 1.3.6.1.4.1.47272.2.9;
- "General terms of contract for provision of trust, information, cryptographic and consulting services with OID: 1.3.6.1.4.1.47272.3.1.2;
- "Tariff for trust, information, cryptographic and consulting services" with OID:1.3.6.1.4.1.47272.2.15;
- "Qualified Trust Service Practice Statement" with OID: 1.3.6.1.4.1.47272.3.1.1;
- "Qualified certificate policy for provision of a qualified electronic signature/seal" with OID: 1.3.6.1.4.1.47272.2.2, 1.3.6.1.4.1.47272.2.3 and 1.3.6.1.4.1.47272.2.2.1;
- "Qualified certificate policy for provision of an advanced electronic signature/seal" with OID: 1.3.6.1.4.1.47272.2.7;
- Policy and Practice of the Time Stamping Authority, Version – 3.0/01.05.2019 with OID: 1.3.6.1.4.1.47272.1.2;
- "Contract for using the services accessible through the application of Evrotrust Technologies AD" with OID:1.3.6.1.4.1.47272.2.16.1;
- "Contract for qualified trust services for clients of Evrotrust Technologies AD – Part 1: Contract with a client that is a natural person" with OID: 1.3.6.1.4.1.47272.2.16.2;

- "Contract for qualified trust services for clients of Evrotrust Technologies AD – Part 1: Contract with a client that is a legal entity" with OID: 1.3.6.1.4.1.47272.2.16.3;
- "Contract for qualified trust services for clients of Evrotrust Technologies AD – Part 2: Contract with a Holder/Creator" with OID: 1.3.6.1.4.1.47272.2.16.4.

1.4.4. VALIDATION SERVICE POLICY

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

1.4.5. VALIDATION SERVICE PRACTICE STATEMENT

The signature validation service (QSVSP) is integrated in this document and has been developed, is applied and updated as specified in ETSI EN 319 401. The SVS Practice Statement describes how Evrotrust implements the service and is owned by the QSVSP. The practice statement is accessible to auditors, users and relying parties. This document describes the method of fulfilment of the requirements that have been identified as necessary to maintain the high quality of the signature validation service. The document has also been endorsed by Evrotrust.

1.4.6. CERTIFICATE USAGE AND APPLICABILITY OF THE VALIDATION SERVICE

Evrotrust offers a service of qualified validation of electronic signatures and seals which allows relying parties to receive a report on the signature/seal validation process in an automated and reliable way. The reports is electronically sealed by Evrotrust and guarantees that signatures and seals are generated and validated in compliance with European legislation (eIDAS).

2. VALIDATION SERVICE MANAGEMENT AND OPERATION

Evrotrust provides cryptographic, information and consulting services related to the validation services applicability, including:

- Issue and operation of qualified certificates for advanced and qualified electronic signatures/seals;
- Issue and operation of website qualified certificates;
- Issue and operation of qualified electronic timestamp;
- Validation of electronic signatures and seals, etc.

Evrotrust provides the services by applying the generally accepted recommendations, specifications and standards. For these services, Evrotrust publishes separate general terms, which are inextricably linked to contractual relations. The policies and practice statements related to the services provided apply to all actors in Evrotrust's public key infrastructure across the world, including certification authorities, registration authorities, commercial representatives, clients, end users and all relying parties.

The certification services are provided in accordance with the Integrated Management System applied by Evrotrust, which incorporates the requirements of ISO 9001, ISO 27001, ISO 22301, ISO 20000-1, Regulation (EU) No. 910/2014. Regulation (EU) No. 2016/679 (GDPR), Directive (EU) No. 2015/2366 (PSD2) and the applicable legislation in the Republic of Bulgaria.

2.1. INTERNAL ORGANISATION

Evrotrust 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 Evrotrust.

In order to achieve reliability and security in its operations related to the provision of trust services, Evrotrust applies the requirements specified in ETSI EN 319 401, including:

- Evrotrust guarantees high level of security and reliability of its operations;
- The trust service practice statements applied by Evrotrust are non-discriminatory;
- The services are available for all entities whose operations fall within the declared

scope of activity and who agree to fulfil their obligations as specified in Evrotrust's general terms;

- Evrotrust concludes a suitable insurance policy every year, in accordance with the applicable law, to cover obligations arising from its operations and in line with Article 13 of Regulation (EU) No. 910/2014;
- Evrotrust has the necessary financial stability and resources for operation in accordance with this document;
- The document "Qualified Trust Service Practice Statement" contains a procedure for resolution of claims and disputes raised by users or relying parties in relation to the provision of the services or other matters related thereto;
- Evrotrust has a documented agreement and contractual relations with third parties, to which it subcontracts services, outsourcing or other activities.

2.1.1. ORGANISATION RELIABILITY

The obligations and responsibilities of the users and Evrotrust are settled by means of contractual agreements. The relations with relying parties are settled according to the terms of the general tort law.

The contracts for provision of trust services shall be signed in a written or electronic form in compliance with the provisions of Regulation (EU) No. 910/2014, Regulation (EU) No. 2016/679 and the applicable law of Republic of Bulgaria. 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.

The qualified validation authority "Evrotrust Qualified Validation Service" of Evrotrust exercises its functions in accordance with the requirements laid down in Regulation (EU) No. 910/2014. The requirements set out the technical and organisational prerequisites for the operations of Evrotrust, the policies for qualified validation and the technical requirements.

In the cases where Evrotrust uses external organisations for support of services or components thereof, they follow the requirements hereunder.

Evrotrust guarantees that:

- it applies operational procedures and security management procedures that

exclude any possibility for manipulation of the validation result/report;

- it checks the validity of the electronic signatures/seals used in line with the requirements of Regulation (EU) No. 910/2014;
- "Evrotrust Qualified Validation Service" checks the validity of the signatures/seals in accordance with ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services.

**The obligations, the responsibilities and the guarantee of the actors in the qualified validation service provision process are described in the document "Qualified Trust Service Practice Statement".*

2.1.2. SEPARATION OF DUTIES

**The duties of Evrotrust, the users and the relying party are described in the document "Qualified Trust Service Practice Statement".*

2.2. HUMAN RESOURCES

Evrotrust applies the requirements specified in clause 7.2 of ETSI EN 319 401.

- Evrotrust guarantees that the employees and contractors observe the requirements for operations reliability;
- Evrotrust hires employees and, if applicable, subcontractors, that have the necessary expertise, reliability, experience and qualification and that have undergone a training on security and personal data protection rules relevant to the operations they perform;
- The employees of Evrotrust undergo periodical (at least every 12 months) training for increasing their expertise, experience and qualification. The trainings include trainings in information security, potential threats and good security practices;
- Proper disciplinary sanctions are imposed on employees who violate the policies of Evrotrust;
- The roles and responsibilities related to information security are documented in the

job descriptions.

- Evrotrust defines reliable roles on which the security of the signatures/seals validation service is based.
- The management of Evrotrust defines the responsibilities of the trusted roles;
- The trusted roles are approved and adopted by the management;
- The employees of Evrotrust (both temporary and permanent) have job descriptions drawn up from the perspective of the roles taken, with separation of duties and the lowest number of privileges, with identification of the position sensitivity based on the obligations and levels of access, the qualification and diploma;
- The job descriptions include requirements for skills and experience and make a distinction between the general and specific duties;
- The employees apply administrative and operational procedures and processes, which are part of the information security management procedures of Evrotrust;
- The management has the necessary knowledge with respect to the trust services provided, knowledge of the security procedures and experience in the field of information security and risk assessment sufficient for fulfilment of management functions;
- All employees of Evrotrust that have trusted roles are free of any conflicts of interests that could affect the objectiveness of the operations of Evrotrust;
- The trusted roles include the following responsibilities:

a) Security officers - overall responsibility for the administration of the application of the security practices;

b) System administrators - they install, configure and support the reliable systems of Evrotrust and the operation of services. This also includes system recovery;

c) System operators - they are responsible for the daily operation of the reliable systems of Evrotrust. They are authorised to execute system backup;

d) System auditors - they are authorised to review and audit the archives and journals of the reliable systems of Evrotrust.

e) Additional roles – there are employees in Evrotrust that fulfil trusted roles for specific trust services.

- The personnel of Evrotrust is assigned trusted roles by the senior management

based on the "lowest privilege" principle with respect to access or during the configuration of the access privileges;

- The personnel is not given access to trusted functions before the necessary verifications take place. Evrotrust requires a certificate of criminal record.

2.3. ASSET MANAGEMENT

2.3.1. GENERAL REQUIREMENTS

Evrotrust applies the requirements specified in clause 7.3 of ETSI EN 319 401. Evrotrust provides high level of protection of its assets, including its information assets. Evrotrust maintains an inventory list of all information assets and classifies them based on the risk assessment.

The service contract, the signature verification status and the signature validation report are linked to the practices, policies and agreements for compliance with other service providers that are outside the control of QSVSP. In this case there may be a delay in the provision of information about a certificate revocation status and it may be necessary for the user to wait for the next CRL in order to ensure that any relevant revocation request has been processed.

The General Terms apply to the policy with OID:1.3.6.1.4.1.47272.2.9.

The rights, obligations and responsibilities of the service actors are described in the document "General terms of contract for provision of trust, information, cryptographic and consulting services" which is an integral part of this document.

Evrotrust provides the applicable policy with OID:1.3.6.1.4.1.47272.2.9 at the following service level (SLA):

The service is available via the website of Evrotrust for personal non-commercial use without any commitment on the part of Evrotrust as to its service level. In order to use the service at the relevant service level or automatically, the client should contact Evrotrust for arrangement of the relationship with an agreement specifying the proposed service level agreement (SLA).

The General Terms describe the options supported by the service.

a) The service allows the user to choose:

- the signed data object (SDO) and the signer's document (SD).

b) The service may allow the user to provide additional details about the validation process:

- the certificates to be used for validation, e.g. in the case where the SDO attributes do not contain the necessary certificates;
- the specific signature that should be verified if the SDO contains multiple signatures; and
- the policy for implicit or explicit signature validation to be used among the available ones.

c) Evrotrust supports the signature formats specified in ETSI EN 319 122-1 and ETSI EN 319 122-2 or in ETSI EN 319 132-1 and ETSI EN 319 132-2 or in ETSI EN 319 142-1 and ETSI EN 319 142-2.

Supported formats with baseline profile of the electronic signature/seal:

- ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI) - XadES Baseline Profile
- ETSI TS 103 173 Electronic Signatures and Infrastructures (ESI) - CadES Baseline Profile
- ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI) – PadES Baseline Profile
- ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI) – AsiC Baseline Profile

In addition, Evrotrust validates the abovementioned formats at an enhanced profile and levels:

- ETSI TS 103 171 Electronic Signatures and Infrastructures (ESI) – XadES-T/TL Level;
- ETSI TS 103 173 Electronic Signatures and Infrastructures (ESI) – CadES T/TL Level;
- ETSI TS 103 172 Electronic Signatures and Infrastructures (ESI) PadES T/TL Level;
- ETSI TS 103 174 Electronic Signatures and Infrastructures (ESI) AsiC T/TL Level.

Evrotrust's validation service validates the following type formats for electronic signature/seal:

- Attached - Enveloped – the electronic signature/seal envelopes the signed object;
- Attached - Enveloping – the signed object envelopes the electronic signature/seal;

- Detached – the electronic signature/seal is outside the signed object – in a separate file/object;
- One document that is electronically signed with more than one electronic signature/seal.

The service successfully validates electronic signatures / stamps with expired or obsolete elements such as expired certificates or time stamps, taking into account during verification the certified date and time of the electronic signature / timestamp. If this time is not certified, the check is done against the present time, and if the validity of the items has expired, this marks the signature as invalid, which is stated in the report. When terminated certificates are used, the service checks whether they were valid at the time of signing, and if not, the service states that the signature as invalid in the report. If an algorithm has been used outside its applicable term, the service states in the report that it's an invalid electronic signature / seal for this reason.

Evrotrust uses cryptographic algorithms in accordance with ETSI TS 119 312, where this information is given by reference to the relevant validation algorithm (ETSI TS 119 102-1).

- SVS selects the validation constraints when the client provides a conflicting indication that contradicts the practice statement of QSVSP;
- QSVSP sets the validation constraints when the signature validation policy provided by the client does not allow this;
- QSVSP indicates in its practice statement how it acts where it is not possible to process the constraints submitted by the client;
- QSVSP determines in its practice statement the conditions under which the signature validation policy may be ignored and replaced by signature validation rules in line with the protocol specified in ETSI TS 119 442, which supports diverse possibilities;
- The SVS policy states what is considered a proof of existence (PoE) of the signature;

2.3.2. OPERATION WITH DIFFERENT MEDIA

All media are stored securely in accordance with the requirements of the information classification scheme. The archives that contain sensitive data are destroyed in a secure manner

when they are no longer necessary.

**The archiving procedure is described in the document "Qualified Trust Service Practice Statement".*

2.4. ACCESS CONTROL

Evrotrust's infrastructure is physically and logically isolated and is not used in any other operations performed by "Evrotrust Technologies" AD. The measures undertaken with respect to Evrotrust's physical protection constitute an element of the Information Security System developed and implemented at Evrotrust, which complies with the requirements of the standards ISO/IEC 27001, ISO 9001, ISO 22301 and ISO/IEC 20000-1. Evrotrust provides physical protection and access control with respect to the premises where the critical components of its infrastructure are installed.

In order to exercise access control, Evrotrust applies the requirements specified in clause 7.4 of ETSI EN 319 401, particularly:

- The access system is limited to authorised individuals;
- Controls (e.g. firewalls) protect the internal network domains of Evrotrust from unauthorised access including access by subscribers and third parties;
- Firewalls are configured to prevent all protocols and accesses not required for the operation of Evrotrust;
- Evrotrust administers user access of operators, administrators and system auditors;
- The administration includes user account management and timely modification or removal of access;
- Access to information and application system functions is restricted in accordance with the access control policy;
- The system of Evrotrust provides sufficient computer security controls. For this purpose, the administration and security management functions are separated. The use of the systems communication channels is restricted and controlled;
- The personnel of Evrotrust is identified and authenticated before using critical

applications related to the service;

- The personnel of Evrotrust is accountable for their activities. For this purpose, the event logs are monitored and retained.
- Sensitive data are protected against being revealed through storage and restriction of access thereto for unauthorised users.

2.5. CRYPTOGRAPHIC CONTROLS

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

- The QSVSP signs the validation reports with a signing 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 for signing the validation reports is stored and used in a cryptographic module (a hardware crypto system/HSM/Hardware Security Module) with level of security FIPS 140-2 Level 3 or higher, or, respectively, CC EAL 4+ or higher.

2.6. PHYSICAL AND ENVIRONMENTAL SECURITY

Evrotrust applies the requirements of clause 7.6 of ETSI EN 319 401 concerning the physical and environmental security. In addition, it applies the following particular requirement of clause 5.2, GSM 1.4 of ETSI TS 119 101 with respect to SVA: Evrotrust uses cryptographic libraries tested against the relevant standard.

**The procedures related to fulfilment of the general requirements with respect to the physical and environmental security are described in the document "Qualified Trust Service Practice Statement".*

2.7. OPERATION SECURITY

Evrotrust applies the requirements specified in clause 7.7 of ETSI EN 319 401 in order to

ensure security of its operations. Evrotrust uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

**Evrotrust applies information security management procedures for the entire infrastructure of Evrotrust in accordance with standard that are generally accepted in international practice, which are described in the document "Qualified Trust Service Practice Statement".*

- Evrotrust performs analysis of security requirements at the design of new systems and new services in order to ensure their security.
- It applies procedures for software change control procedures and control on the change of the technological systems configuration;
- The change control procedures include their documentation;
- The integrity of the systems and information of Evrotrust are protected against viruses, malicious and unauthorised software;
- The media used within the systems of Evrotrust are securely handled to protect the archives from damage, theft, unauthorised access and obsolescence;
- The media management procedures protect against obsolescence and deterioration of their condition within the period of time that records are required to be retained;
- The procedures are applied by all trusted and administrative roles that impact on the provision of services;
- Evrotrust specifies and applies procedures for ensuring that:

a) security patches are applied within a reasonable time after they come available;

b) security patches are not applied if they may introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them;

c) the reasons for not applying any security patches are documented.

In addition, the following specific operation security requirements are applied:

- Evrotrust uses the latest and up-to-date environment for applications (operated software environment);

- Positively tested and reviewed realisations of standardised protocols and libraries are used;
- The SCA / SVA / SAA maintains the integrity and confidentiality of the entire information provided by any user, as well as of any data transmitted between the application and the user, even in the case of an application with a publicly accessible environment.

2.7.1. INFORMATION SECURITY POLICY

Evrotrust has developed an Information Security Policy which is approved by the management in accordance with the requirements of clause 6.3 of ETSI EN 319 401:

- The policy defines Evrotrust's approach in the management of its information security operations;
- Any changes to the information security policy are communicated to third parties (subscribers, relying parties, supervisory or other regulatory bodies, compliance assessment bodies), where applicable.
- Evrotrust's information security policy is documented, implemented and maintained up-to-date;
- All employees of Evrotrust have been familiarised with the Information Security Policy;
- Evrotrust is responsible for observation of the procedures described in the Information Security Policy in the cases where it subcontracts part of its operations. If there are subcontractors, Evrotrust defines their liability and ensures that they are bound to strictly apply all information security controls required by Evrotrust;
- The policy for information security of Evrotrust and inventory of assets for information security assets are reviewed at planned intervals from time to time or in the case of significant changes in order to ensure their continuing suitability, adequacy and effectiveness;
- Any changes that will impact on the level of security provided are approved by the information security management body;
- The configuration of the systems of Evrotrust is regularly checked for changes which violate the information security rules. The maximum interval between two validations is

based on the internal procedures of Evrotrust.

In addition, the following specific requirements are applied:

The security policy documents the security controls and the data privacy controls. The personal data provided to Evrotrust are stored and processed in accordance with the Personal Data Protection Act and REGULATION (EU) 2016/679 - General Data Protection Regulation (GDPR). Evrotrust collects a proportionate quantity of information to its purpose and use. Each user provides their consent to the processing of personal data. This consent is declared by signing the Contract for trust services. The personal data are only used in relation to the provision of the specific trust service. The personal data are protected in accordance with the privacy rules contained in Evrotrust's security policy.

2.8. NETWORK SECURITY

Evrotrust applies the requirements specified in clause 7.8 of ETSI EN 319 401.

**Evrotrust guarantees its systems network security from external attacks and threats by applying the procedures described in the document "Qualified Trust Service Practice Statement".*

In addition, the following particular requirements are applied:

- In case remote access to systems storing or processing confidential data is allowed, a policy for documenting the security and confidentiality controls implemented for the purpose of personal data protection is followed.
- In case remote access to systems storing or processing confidential data is allowed, appropriate security measures are undertaken to protect against the risks of remote access. NOTE: This confidential information can be subscriber related information (like preferences), or signed data that would be stored waiting further processing (e.g. if revocation status data is unavailable).

2.9. INCIDENT MANAGEMENT

2.9.1. RISK ASSESSMENT

In order to ensure the quality and reliability of the services provided, Evrotrust regularly performs risk assessment. The security checks defined in the security concept of the Provider are controlled on a quarterly basis in order to ensure effectiveness of control.

Evrotrust applies the requirements specified in clause 5 of ETSI EN 319 401 with respect to risk assessment:

- Evrotrust carries out a risk assessment to identify, analyse and evaluate the risks associated with the business and the technical issues in the trust service provided;
- Evrotrust selects appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures ensure that the level of security is commensurate to the degree of risk;
- Evrotrust determines all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the practice statement;
- The risk assessment is regularly reviewed;
- The management of Evrotrust approves the risk assessment and accepts the residual risk identified.

2.9.2. INCIDENT MANAGEMENT

All systems involved in the issue of a qualified electronic timestamp offer a high level of reliability. The technological system is located in a physically protected environment which minimises the risk of natural disasters.

**The procedures and plans for achieving continuity and security in the Provider's operations are described in the document "Qualified Trust Service Practice Statement" of Evrotrust Technologies AD.*

For incident management, Evrotrust applies procedures that fulfil the requirements specified in clause 7.9 of ETSI EN 319 401:

- Evrotrust monitors all activities concerning access to and use of information systems and service requests;
- The monitoring activities take into account and analyse the sensitivity of any information collected;
- Abnormal system activities that indicate a potential security violation, including intrusion into Evrotrust's system and network are detected and reported as alarms;
- Evrotrust monitors the following events:

  a) start-up and shutdown of the logging functions; and

  b) availability and utilisation of needed services with Evrotrust's network.
- Evrotrust acts in a timely and coordinated manner in order to respond quickly to incidents

and to limit the impact of breaches of security;

- Evrotrust appoints trusted role personnel to follow up on alerts of

potentially critical security events and ensure that relevant incidents are reported in line with the established internal procedures;

- Evrotrust has established procedures to notify the relevant competent authorities in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service and on the personal data within 24 hours of the breach being identified.
- Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, Evrotrust notifies the relevant natural or legal person of the breach of security or loss of integrity without undue delay;
- Evrotrust's systems are regularly monitored to identify evidence of malicious activity by implementing automatic mechanisms to process the audit logs and the personnel is alerted of possible critical security events;
- Evrotrust announces any critical vulnerability not previously announced within a period of 48 hours after its discovery;

- For each vulnerability, considering its potential impact, Evrotrust:
  - creates and implements a plan to mitigate the vulnerability; or
  - documents with evidence any determination that the vulnerability does not require remediation, e.g. if the costs of its potential impact do not justify the costs for its mitigation;
- Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimised.

2.10. COLLECTION OF EVIDENCE

Evrotrust applies the requirements specified in clause 7.10 of ETSI EN 319 401 with respect to collection of evidence.

- Evrotrust records and keeps accessible for an appropriate period of time, including after its activities have ceased, all relevant information concerning data issued and received during the activity, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service;
- The confidentiality and integrity of current and archived records concerning operation of services is maintained;
- Records concerning the operation of services are completely and confidentially archived in accordance with the good business practices;
- Records concerning the operation of services are made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings;
- The precise time of significant operation management events, such as key management and clock synchronisation, are recorded;
- The time used to record events as required in the audit log is synchronised with UTC at least once a day;
- Records concerning services are held for a certain period of time as appropriate for providing the necessary legal evidence and as notified in the General Terms and the contract;
- The events are logged in a way that they cannot be easily deleted or destroyed

(except if reliably transferred to long-term archives) within the period of time that they are required to be held.

In addition, the following particular requirements are applied:

- The QSVSP shall implement event logs to capture information needed for later proofs;
- Any signature validation is logged, possibly together with the identification of the subscriber when this information is known. As a standard, Evrotrust does not log the identity of the subscriber;
- Event logs are marked with a timestamp;
- The archived data (on paper and in electronic format) are stored for a period of no less than 10 years. After expiration of this period the archived data are destroyed;
- The event log includes the 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.

**Additional information on the archive data and evidence collection is described in the document "Qualified Trust Service Practice Statement".*

2.11. BUSINESS CONTINUITY MANAGEMENT

Evrotrust applies the requirements specified in clause 7.11 of ETSI EN 319 401 with respect to business continuity management.

- Evrotrust has defined and maintains a continuity plan to enact in case of a disaster.
- In the event of a disaster, including failure of the technological system, including the hardware and software, compromise of a private signing key or compromise of some other keys, the operations are restored within the delay established in the continuity plan, having addressed any cause for the disaster in order to prevent its recurrence.

In order to ensure business continuity, further particular requirements for the service are applied:

- The business continuity plan, the plan for recovery after a disaster, etc. are

described in procedures used for exercising all reasonable efforts to keep the service available in line with the Service-Level Agreement (SLA), and the necessary technical and organisational precautions are undertaken to ensure this alignment.

- Measures should be implemented to avoid interruption by third parties or unintentional interruptions by the user.
- When validation reports are digitally signed and expected to be validated over the long term, the QSVSP signs with a certificate for an electronic seal issued by a certification authority that provides guarantees on the availability of the information on the status of its certificates and that has an activity termination plan;
- When validation reports are digitally signed and expected to be validated over the long term, the QSVSP selects a trusted source for proofs of existence. In the specific case, Evrotrust uses a qualified authority for the timestamp.

**The possible causes for accidents and the implementation of the continuity plan are detailed in the document "Qualified Trust Service Practice Statement".*

2.12. TERMINATION PLANS FOR THE ACTIVITY OF EVROTRUST

The obligations described below have been developed in order to minimise any interruptions in the users' and relying parties' operations as a result of Evrotrust's decision to terminate its activity. In its termination plans for its activity, Evrotrust applies the procedure that fulfils the requirements specified in clause 7.12 of ETSI EN 319 401:

- The potential interruptions for users and relying parties caused by the termination of Evrotrust's services are minimised and, particularly, the information necessary for validation of the trust services continues to be supported;
- Evrotrust periodically updates the termination plan. Before Evrotrust terminates its services, at least the following procedures apply:
  - Evrotrust informs the following of the termination of its activity: all subscribers and other stakeholders with which it has agreements or other form of established relations, among which relying parties, the relevant competent authorities such as supervisory bodies;

- Before terminating its services, Evrotrust terminates the authorisation of all subcontractors to act on their behalf in carrying out any functions relating to the process of issuing trust service certificates/tokens and/or reports;
- Before terminating its services, Evrotrust transfers its obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the services for a reasonable period, unless it can be demonstrated that Evrotrust does not hold any such information;
- Before terminating its services, the private keys of Evrotrust, including backup copies, are destroyed or withdrawn from use, in a manner such that the private keys cannot be retrieved;
- Before terminating its services, where possible, Evrotrust transfers the provision of trust services for its existing customers to another qualified trust service provider;

➢ Evrotrust has an arrangement to cover the costs to fulfil these minimum requirements in case of bankruptcy or if it is unable to cover the costs by itself for other reasons, as far as possible within the constraints of applicable legislation;

➢ Evrotrust maintains or transfers to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.

**The plans and procedures for termination of the activity of Evrotrust are described in the document "Qualified Trust Service Practice Statement".*

2.13. COMPLIANCE

Evrotrust applies the requirements specified in clause 7.13 of ETSI EN 319 401 in order to ensure compliance with the legal requirements.

➢ Evrotrust guarantees that it operates in a legal and trustworthy manner;

➢ It provides evidence on how it meets the applicable legal requirements;

➢ The trust services provided and the end user products used in the provision of those services are made accessible for persons with disabilities, where possible;

➢ Evrotrust takes due consideration of all applicable standards in its activity, such as

ETSI EN 301 549 Accessibility requirements suitable for public procurement of ICT products and services in Europe;

- 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. Evrotrust guarantees that personal data are processed in accordance with Regulation (EU) No. 2016/679. In this respect, authentication for a service online concerns processing of only those identification data which are adequate, relevant and not excessive.

In addition, the following specific requirements are applied:

- When personal data is processed by a third party, Evrotrust signs an appropriate agreement for processor of personal data in order to ensure that it complies with the requirements stated in the QSVSP practice statements and terms and conditions, including with regard to the implementation of technical, organisational and legal measures to protect the personal data (where both signed data and the signature itself may contain personal data);
- QSVSP does not store the signer's document (SD) after processing when not necessary. If the validation service works in combination with a long-term preservation service, such data may need to be kept;
- The QSVSP has the overall responsibility for meeting the requirements defined above when some or all of its functionalities are undertaken by subcontractors.

The service is provided in accordance with the requirements for qualified validation of qualified electronic signatures set out in Regulation (EU) No. 910/2014 (eIDAS: Art. 32 and 33) and seals (eIDAS: Art. 40)

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	The qualified electronic signature validation process fulfils the EU requirements for qualified trust service provider that issues

that: a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;	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	The service verifies whether the advanced

were met at the time of signing.	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	The service also covers the validation of electronic seals within the meaning of Art. 40.

qualified electronic seals.	

3. SIGNATURE VALIDATION SERVICE DESIGN

3.1. VALIDATION PROCESS REQUIREMENTS

The validation process complies with ETSI TS 119 102-1. QSVSP implements the algorithm specified in ETSI TS 119 102-1 by allowing allows alternative implementations provided that they produce the same main status indication when given the same set of input information.

In particular, Evrotrust 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 been signed indirectly); • any constraints applicable to the signer's identity certification have been positively validated (i.e. the signing certificate has been found trustworthy); and • the electronic signature/seal has been

		positively validated against the validation constraints and hence is considered conformant to these constraints.
TOTAL-FAILED	The validation process outputs additional information to explain the TOTAL-FAILED indication for each of the validation constraints that have been taken into account and for which a negative result occurred.	The qualified electronic signatures and seals validation process results into TOTAL-FAILED because the cryptographic checks of the electronic signature/seal failed (including checks of hashes of individual data objects that have been signed indirectly) or it has been proven that the generation of the signature/seal took place after its revocation.
INDETERMINATE	The validation process outputs additional information to explain the INDETERMINATE 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 semantics:

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	The electronic signature/seal is not compatible with the standards supported specified in this document to a level that prevents the cryptographic check

		signature/seal.	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 outputs the 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 signature/seal. • CRL, if any, for which the revocation has been established.	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 signature/seal lies after the revocation time.
INDETERM	SIG_CONSTR	The validation process provides	The qualified validation process

INATE	AINTS_FAILURE	multiple reasons that have resulted in unsuccessful validation.	of electronic signatures and seals results into INDETERMINATE because one or more attributes of the electronic signature/seal do not match the validation constraints.
	CHAIN_CONSTRAINTS_FAILURE	The validation process provides the following: • The certificate chain used in the validation process. • Additional information on the cause that has led to this result.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the certificate chain used in the validation process does not match the validation constraints related to the certificate.
	CERTIFICATE_CHAIN_GENERAL_FAILURE	The validation process provides additional information on the reason for this result.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the validation of the certificate chain has produced an error for an unspecified reason.
	CRYPTO_CONSTRAINTS_FAILURE	The validation process provides identification of an electronic signature/seal or of a certificate generated using an algorithm or key size below the required cryptographic security level.	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).
	EXPIRED	The validation process provides data about the validated certificate chain.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because time of placing the electronic signature/seal lies after the expiration date (notAfter) of the certificate.
	NOT_YET_VALID	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because time of placing the electronic signature/seal lies

			before the expiration date (notBefore) of the certificate.
	POLICY_PROCESSING_ ERROR	The validation process provides additional information on the reason.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the given formal policy file could not be processed for any reason (e.g. not accessible, not pursuable, digest mismatch, etc.).
	SIGNATURE_POLICY_N OT_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.
	TIMESTAMP_ORDER_ FAILURE	The validation process outputs a list of timestamps that do no respect the ordering constraints.	The qualified validation process of electronic signatures and seals results into INDETERMINATE the provided list of timestamps and/or signed data object(s) do not respect the constraints on the order.
	NO_SIGNING_CERTIFICATE_FOUND	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the certificate for electronic signature/seal cannot be identified.
	NO_CERTIFI	-	The qualified validation process

	CATE_CHAIN_FOUND		of electronic signatures and seals results into INDETERMINATE because no certificate chain has been found for the identified certificate for electronic signature/seal.
	REVOKED_NO_POE	The validation process provides the following: •The certificate chain used in the validation process. • The time and the reason of revocation of the certificate for electronic signature/seal.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the corresponding certificates has been revoked during the validation. However, it may not be established whether the signature time lies before or after the revocation time.
	REVOKED_CA_NO_POE	The validation process provides the following: •The certificate chain which includes the revoked certification authority certificate; • The time and the reason of revocation of the certificate.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because at least one certificate chain was found but an intermediate certification authority is revoked.
	OUT_OF_BOUNDS_NO_POE	-	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the certificate is expired or not yet valid at the validation date/time and the SVA cannot ascertain that the signing time lies within the

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

			because not all constraints can be fulfilled using available information. However, the process may be possible if the validation uses additional revocation information that will be available at a later point of time.
	SIGNED_DATA_NOT_FOUND	The validation process provides the following: The identifier (e.g. an URI) of the signature/seal data that caused the failure.	The qualified validation process of electronic signatures and seals results into INDETERMINATE because the data about the signature/seal cannot be obtained.
	GENERIC	The validation process provides additional information showing why the validation indication is INDETERMINATE.	The qualified validation process of electronic signatures and seals results into an INDETERMINATE because of other reasons.

- Evrotrust supports at least one signature validation policy as an input 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 possibilities;
- 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

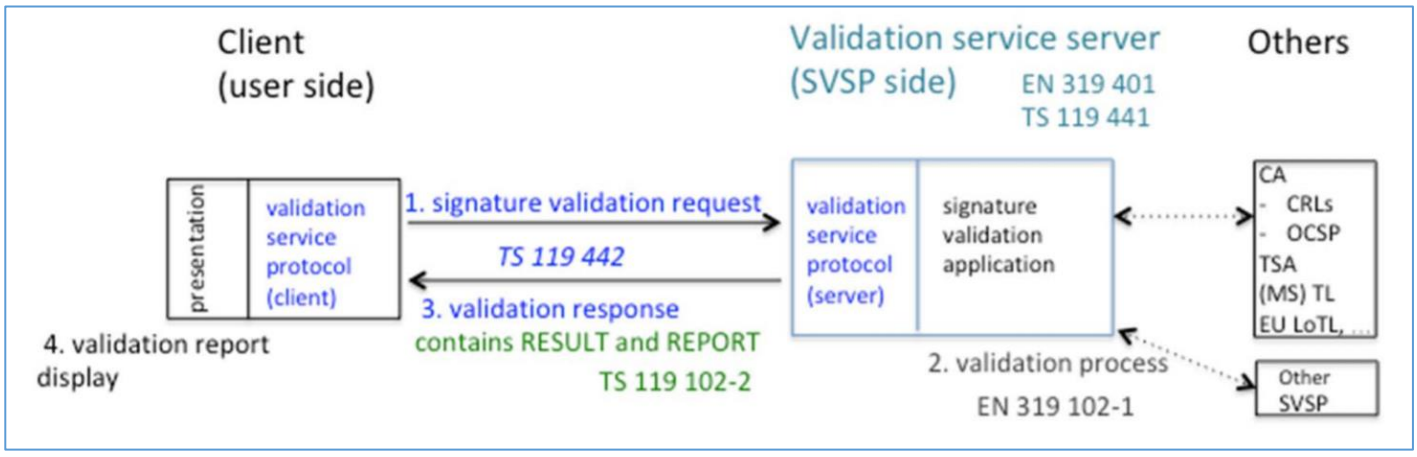
the SVS;

- 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. Evrotrust 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,

Evrotrust restricts the validation only to the parameters described therein.

QSVSP does not support signature validation policies provided by a 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. Evrotrust 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 signed with a qualified certificate for qualified electronic seal.
- 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. In addition, there may be constraints related to the used certificates for electronic signature/seal. It is also possible to submit a formal policy specification to be applied at the time of validation. Specific restrictions and/or extensions for a given trusted party may also be agreed for the validation of reports provided to them. 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, which shall not exceed 10 megabytes. In

addition, during the validation process a qualified time stamping service of Evrotrust 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 Union Trusted List of Trust Service Providers** https://webgate.ec.europa.eu/tl-browser

(m) 1.2 *CertificationPath*: This constraint indicates a certification path required to 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 considering the 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)	**None**
➢ (m) 1.4. *initial-policy-mapping-inhibit*: According to IETF RFC 5280, clause 6.1.1 (e)	**None**
➢ (m) 1.5. *initial-explicit-policy*: According to IETF RFC 5280, clause 6.1.1 (f)	**None**
➢ (m) 1.6. *initial-any-policy-inhibit*: According to IETF RFC 5280, clause 6.1.1 (g)	**None**
➢ (m) 1.7. *initial-permitted-subtrees*: According to IETF RFC 5280, clause 6.1.1 (h)	**None**
➢ (m) 1.8. *initial-excluded-subtrees*: According to IETF RFC 5280, clause 6.1.1 (i)	**None**
➢ (m) 1.9. *path-length-constraints*: This constraint concerns the number of certificates 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 or not 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 certificate for electronic signature/seal used in validating the signature/seal to be issued by a CA that keeps the renewals of revoked certificates even after they have expired for a period exceeding a given lower bound.	**None**

(m) 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:	**None**
• EUQualifiedCertificateRequired	Yes
• EUQualifiedCertificateSigRequired	Yes
• EUQualifiedCertificateSealRequired 1	Yes

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** **None** **None** **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 QSVSP may conform to 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. The communication channel between the QSVSP and other TSP is outside the scope of this document.

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 OASIS DSS interface defines the validation interface for one or more documents signed with an electronic signature/seal. Both protocols of the OASIS DSS use SOAP transport protocol for exchange of the XML commands during the signature/seal validation. The specifications of the DSS interface are regulated and maintained by the OASIS consortium.

The service is accessed and used through a web interface. In this interface the XML commands of the DSS interface use HTTP POST for exchange/transport. The client accesses the service and may indicate and load a document signed with an electronic signature/seal, choose the parameters of the request and then sent the formed Service Request via HTTP POST protocol.

3.3.1. COMMUNICATION CHANNEL

The QSVSP offers a secure communication channel and guarantees the confidentiality of the authentication process and users' personal data. The QSVSP 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 Evrotrust (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 Evrotrust 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 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 different sources:

- 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; or
- a local source from the verifier (e.g. configuration file, machine processable signature validation policy).

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 Evrotrust;
- 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 electronic seal of Evrotrust;
- 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 Evrotrust's website, validation takes place in a TLS session.

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

This document has been published on Evrotrust's website on the internet in Bulgarian and in English language. In case of any discrepancy between the Bulgarian and the English text, the Bulgarian text takes precedence.