QUALIFIED PRESERVATION SERVICE

FOR QUALIFIED ELECTRONIC SIGNATURES / SEALS

POLICY AND PRACTICE

CONTENTS

1 INTRODUCTION

Evrotrust Technologies AD (Evrotrust) is a qualified provider of qualified trust services performing its business in accordance with the requirements of Regulation (EU) No. 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Regulation (EU) No. 910/2014) and the Electronic Document and Electronic Trust Services Act (EDETSA) and, as such, it is registered in the trusted list of the European providers of trust services (https://webgate.ec.europa.eu/tl-browser/#/tl/BG), as well as in the register of the Bulgarian trust services providers maintained by the Communications Regulation Commission (CRC) (БЪЛГАРИЯ (BULGARIA) - Trusted List ID: BG_TSL (crc.bg)).

Evrotrust provides its users with a highly reliable and secure service for qualified preservation of qualified electronic signatures/seals in compliance with Art. 34 (1) and Art. 40 of Regulation (EU) No. 910/2014.

Regulation (EU) No. 910/2014 states that the qualified preservation service refers to qualified electronic signatures/seals and not to data preservation in general, but no provision prohibits other data to be preserved by the service as well. In this sense Evrotrust takes the chance to preserve any documents with no limitations to their type and contents. The necessity of long-term preservation (with storage) is acknowledged in Regulation (EU) No. 910/2014 i. (61) emphasizing that Regulation (EU) No. 910/2014 should ensure the long-term preservation (with storage) of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes. These are the grounds the service for qualified preservation of qualified electronic signatures/seals offered by Evrotrust is based on.

Evrotrust guarantees that, complying with the requirements of this document, it ensures lawful processing of the personal data of any persons related to the provision of a service for qualified preservation of qualified electronic signatures/seals to any persons using the service, providers, any third parties, etc., if any, in accordance with Art. 24 (2) of Regulation (EU) No. 910/2014 and Regulation (EU) 2016/679 (GDPR).

The service for qualified preservation of qualified electronic signatures/seals (QPSES) ensures secure and reliable long-term preservation (with storage) of any type of documents of the submitters and provide evidence of the preservation process.

1.1 OVERVIEW

"Qualified preservation service for qualified electronic signatures/seals policy and practice"(the Policy&Practice) is a document describing the general rules and standards applied by Evrotrust Technologies AD (Evrotrust) while providing the qualified preservation service for qualified electronic signatures/seals (QPSES).

This document refers to a trust service provided by Evrotrust pursuant to Art. 34 (1) and Art. 40 of Regulation (EU) No. 910/2014 and in compliance with the applicable legislation of the Republic of Bulgaria. The Policy&Practice describes all requirements related to any used procedures and technologies that could enhance the reliability of the qualified electronic signature/seal outside its technological validity period. Evrotrust applies the requirements, recommendations or authorizations of the European Commission applicable to a service for qualified long-term preservation with storage (preservation service with storage) for combined preservation of digital signatures and with temporary storage (preservation service with temporary storage) for any type of data objects.

This document sets out the common applicable requirements, stated in the ETSI EN 319 401 Standard, to the business of Evrotrust as a qualified trust service provider. The Policy&Practice determines requirements for Evrotrust's security regards ensuring long-term preservation of the digital signatures/seals and general data, i.e. signed or unsigned data, as well as techniques.

The service is intended for natural and legal persons, for administrations, for persons performing public functions and for organisations providing public services. The relationship between Evrotrust and the end-user are governed by the General Terms and Conditions of the Contract for Trust, Information, Cryptographic and Other Services, or, where applicable, by a contract for provision of the respective service, the General Terms being an inseparable part thereof.

The price of QPSES provision is stated in the "Tariff for certification, information, cryptographic and consulting services" accessible on the Evrotrust website (https://www.evrotrust.com) in the Documents section.

The Policy&Practice is a public document. It may be amended by Evrotrust at any time, and each new version is approved by the Board of directors and announced to the persons concerned through the company website (https://www.evrotrust.com).

1.1.1 NORMATIVE REFERENCES

The Policy&Practice complies with the following normative documents, standards, standardization documents and recommendations:

- Regulation (EU) No. 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- Regulation (EU) 2016/679 of the European Parliament and 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 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI SR 019 510 Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures;
- ETSI TR 119 001 Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations;
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites;
- ETSI EN 319 102-1 Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation;
- 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 TS 119 122-3 Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES;

- 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 EN 319 162-1 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers;
- ETSI EN 319 162-2 Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers;
- 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 EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles;
- ETSI TS 119 512 Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services;
- ISO 14721 Space data and information transfer systems -- Open archival information system (OAIS) - Reference model;
- ISO/IEC 21320-1 Information technology -- Document Container File -- Part 1: Core;
- IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP);
- IETF RFC 3986 Uniform Resource Identifier (URI): Generic Syntax;
- IETF RFC 4998 Evidence Record Syntax (ERS);
- IETF RFC 5280 Public Key Infrastructure Certificate and Certificate Revocation List

(CRL) Profile;

- IETF RFC 5816 ESSCertIDv2 Update for RFC 3161;
- IETF RFC 6283 Extensible Markup Language Evidence Record Syntax (XMLERS);
- IETF RFC 6838 Media Type Specifications and Registration Procedures;
- IETF RFC 6960 Online Certificate Status Protocol – OCSP;
- W3C Extensible Markup Language (XML) 1.0 (Fifth Edition)", W3C Recommendation;
- BSI TR-03125-F Preservation of Evidence of Cryptographically signed Documents, Formats (TR-ESOR-F);
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- ETSI TS 119 441 Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services;
- ETSI TS 119 442 Electronic Signatures and Infrastructures (ESI);Protocol profiles for trust service providers providing AdES digital signature validation services.

1.2 NAME AND AND IDENTIFIER OF THE DOCUMENT

The full name of this document is "Qualified preservation service for qualified electronic signatures/seals (QPSES) (Qualified preservation service) Practice and Policy of Evrotrust Technologies AD" and object identifier (OID):

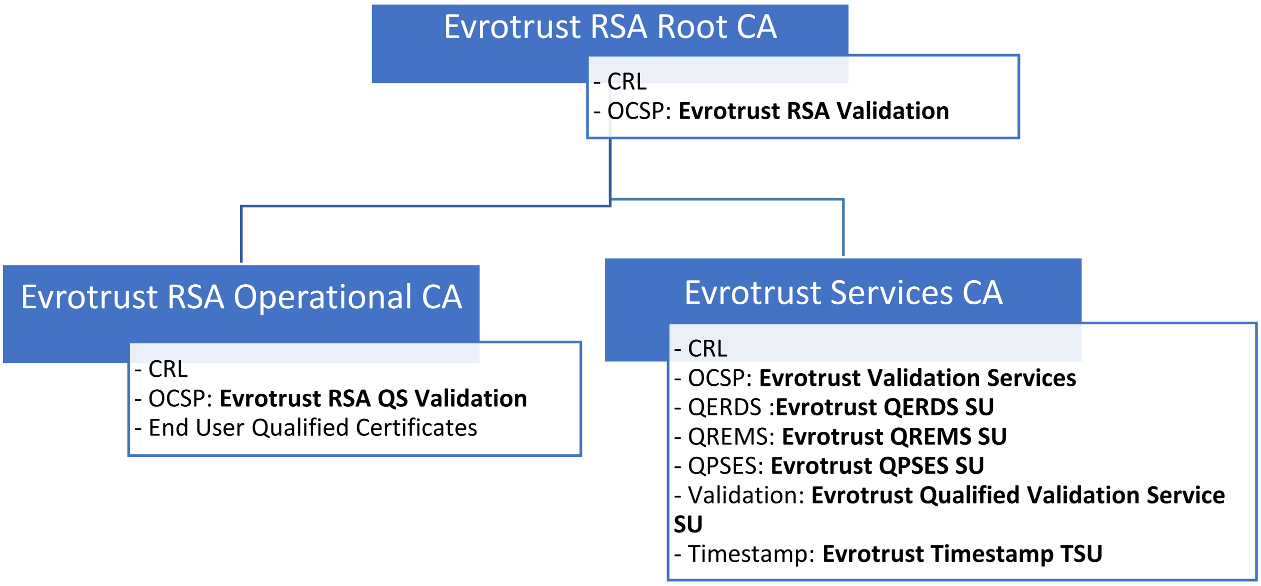
Name of the document	Object Identifier (OID)
QUALIFIED PRESERVATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES/SEALS PRACTICE AND POLICY	1.3.6.1.4.1.47272.2.13

Evrotrust ensures that it does not change 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.

1.3 PARTICIPANT IN THE INFRASTRUCTURE

1.3.1 CERTIFYING AUTHORITIES

The hierarchy of the certification authorities of Evrotrust is described in item 1.5.1.1 of the document entitled "Certification Practice Statement for Qualified Trust Services"


Evrotrust RSA Root CA
- CRL
- OCSP: **Evrotrust RSA Validation**
Evrotrust RSA Operational CA
- CRL
- OCSP: **Evrotrust RSA QS Validation**
- End User Qualified Certificates
Evrotrust Services CA
- CRL
- OCSP: **Evrotrust Validation Services**
- QERDS :**Evrotrust QERDS SU**
- QREMS: **Evrotrust QREMS SU**
- QPSES: **Evrotrust QPSES SU**
- Validation: **Evrotrust Qualified Validation Service SU**
- Timestamp: **Evrotrust Timestamp TSU**

1.3.1.1 ROOT CERTIFYING AUTHORITY ("EVROTRUST RSA ROOT CA")

Evrotrust RSA Root CA issues qualified electronic certificates that are hierarchically dependent on infrastructure in the Evrotrust domain. The basic certificate of Evrotrust is self-issued and self-signed with the Evrotrust basic private key. With the base private key, the provider signs public key certificates to its operational Certification Authorities.

1.3.1.2 OPERATIONAL CERTIFIED AUTHORITY (EVROTRUST SERVICES CA)

"Evrotrust Services CA" is the certifying authority of the qualified preservation service for qualified electronic signatures / seals (QPSES) which, by using the signing unit "Evrotrust QERDS SU", electronically signs the evidence issued under this policy.

1.3.1.3 CERTIFICATE STATUS AUTHORITY (EVROTRUST SERVICES VALIDATION)

"Evrotrust Services Validation" is the validating authority of the qualified preservation service for qualified electronic signatures / seals (QPSES) which signs the status certificates issued by Evrotrust Services CA. The status verification service is accessed via OCSP protocol.

1.3.1.4 THE AUTHORITY FOR THE ISSUANCE OF QUALIFIED ELECTRONIC TIMESTAMP "EVROTRUST TSA"

"Evrotrust TSA" is a certifying authority within the Evrotrust structure that provides a qualified TSS time verification service. "Evrotrust TSA" accepts queries for the issuance of qualified electronic time stamps to verify accurate time in the generated evidence.

A detailed description is provided in the document "Policy and practice of qualified electronic time stamps service".

1.3.2 REGISTRATION AUTHORITY

Evrotrust users are initially identified through a reliable, secure and certified infrastructure. The electronic video identification scheme for natural and legal persons via a mobile device complies with the requirements of Regulation (EU) No. 910/2014.

The Registration Authority is a separate structure of Evrotrust but may also be an external party to whom Evrotrust assigns the performance of services of verification of the registration, identification and authentication of QERDS users.

Contact details of the Evrotrust Registration Authority are available on the company's website (e-mail: office@evrotrust.com, tel.: 02 448 58 58).

1.3.3 USERS

Any natural or legal person who has a contract with Evrotrust for a qualified preservation service for qualified electronic signatures / seals is a QERDS user.

Where practically feasible, the certification service provided and the products used in the QERDS delivery are also accessible to people with disabilities.

1.3.4 TRUSTING PARTIES

Trusting parties (third parties) are natural or legal persons who rely on the evidence provided by the provider in relation to the QERDS.

In this case, they are not QERDS users.

1.3.5 OTHER PARTICIPANTS

To provide the service under this document, Evrotrust does not use external qualified certification service providers. Evrotrust reserves the right to enter into contracts with external parties for the provision of certain certification services, where necessary.

1.4 APPLICABILITY OF QUALIFIED PRESERVATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES / SEALS

The service is intended for users who need long-term preservation of their electronic documents or long-term preservation of documents signed with electronic signature. Preservation Service aims to support a qualified preservation service for qualified electronic signatures / seals under Regulation (EU) No 910/2014.

This document deals with two main applications:

1) Long-term preservation using electronic signature techniques, the ability to validate an electronic signature, the ability to maintain its validity status, and the ability to obtain evidence of the existence of associated signature data, as well as during the filing preservation service, even if later the signature key is compromised, the validity of the certificate expires or there is cryptographic attack of the signature algorithm or hash algorithm used in the signature;
2) Provide evidence of the existence of digital objects, no matter signed or not, using electronic signature techniques (electronic signatures, time stamps, records of evidence, etc.).

1.5 POLICY&PRACTICE MANAGEMENT

1.5.1 ORGANISATION MANAGING THE POLICY&PRACTICE

Evrotrust has a reliable and secure organizational structure. Evrotrust is responsible for the management of this Policy&Practice. Each Policy&Practice version is effective by the approval and publishing of a new version. Each new version is elaborated by employees of Evrotrust and published following the approval of the Board of Directors of Evrotrust.

The users have the obligation to comply with the valid Policy&Practice version only as of the time of using Evrotrust's services. Evrotrust provides its service to all persons whose activities fall within its stated field of application and who agree to abide by the obligations set out in this document.

1.5.2 CONTACT PERSON

The contact person for managing the document "Qualified preservation service for qualified electronic signatures/seals policy of Evrotrust Technologies AD" is the Executive director of Evrotrust.

Additional information may be obtained at the following address:

Evrotrust Technologies AD
Sofia, 1766
Business center MM, floor 5, "Okolovrasten pat" 251G
Phone, fax: + 359 2 448 58 58 – information/registration authority/technical support
email address**:** office@evrotrust.com
web site: http://www.evrotrust.com

1.6 DEFINITIONS AND ABBREVIATIONS

1.6.1 DEFINITIONS

QPSES (Preservation Service for Electronic Signatures): a qualified preservation service for qualified electronic signatures/seals;

OCSP: a protocol providing online certificate status information (OCSP or CRL);

Container: a data object which contains a set of data objects and additional information describing the contained data objects and optionally its content and its interrelationships (digital signatures/seals, time-stamps, evidence records, validation data, etc.);

Delta preservation object container: a preservation object container describing exclusively the difference between an already existing preservation object container and an updated data object;

digital signature techniques: techniques based on digital signatures/seals, time-stamps or evidence records;

EU qualified time-stamping authority: a qualified trust service provider issuing qualified electronic time-stamps as laid down in Regulation (EU) No. 910/2014;

evidence record: data that can be used to prove the existence of an archived data object or an archived data object group at a certain time;

expected evidence duration: expected duration of the evidence records;

export-import package: information extracted from the preservation service, including content and evidence, that can be imported;

long-term: a long time period in which technological changes, such as obsolescence of cryptographic technology, crypto algorithms, key sizes or hash functions, key compromises or the ability to check the validity status of the certificates may be a concern;

long-term preservation: long-term preservation (with storage), where the extension of the validity status of a digital signature and / or the provision of proofs of existence of data over a long period of time does not depend on the obsolescence of cryptographic technology, crypto algorithms, key sizes or hash functions, key compromises or the ability to check the validity status of the certificates;

notification protocol: a protocol used by the preservation service to notify the preservation client;

preservation client: a preservation client being a component or a piece of software which interacts with a preservation service via the preservation protocol;

preservation evidence: evidence of preservation provided by the preservation service which can be used to prove that one or more preservation goals are met for a given object;

preservation evidence policy: an evidence preservation policy, including a set of rules specifying

the requirements and the internal process of generating and validating any preservation evidence;

preservation evidence retention period: a preservation period of preservation evidence;

preservation goal: the preservation goal is the extension (augmentation) of the validity status of digital signatures/seals beyond the technological validity status, provision of proofs of existence of data over long periods of time or a combination of both;

preservation mechanism: preservation mechanism based on digital signature techniques, which is used to preserve preservation objects and to maintain the validity of preservation evidence**;**

preservation interface: the preservation interface is a component implementing the preservation protocol. Evrotrust elaborates and uses an applied programming interface (API) in compliance with the requirements of ETSI TS 119 512;

preservation manifest: description of a data object in a preservation container referring to the preservation data objects or additional information and metadata in the preservation object container;

preservation object: a preservation object, which is submitted to, processed by or retrieved from a data preservation service;

preservation object container: a container for data object preservation, for example, ASiC-S, ASiC-E or Information Packages OAIS;

preservation object identifier: a unique identifier of a preservation object;

preservation period: a preservation period has the duration in which the preservation service preserves the submitted preservation objects and any evidence associated there to;

preservation profile: a preservation profile represents a uniquely identified set of implementation details pertinent to the preservation storage model and the preservation goals which specify how preservation evidence is generated and validated;

preservation protocol: communication protocol between the preservation service and the client;

preservation scheme: a preservation scheme represents a set of procedures and rules pertinent to the preservation storage model and the preservation goals;

preservation service: a preservation service capable of extending the validity status of a digital signature over a long period of time and / or providing proofs of existence data over a long period of time;

preservation service provider: a provider rendering a preservation service;

preservation service policy: a policy for a preservation service;

preservation service practice statement: a practice statement for a preservation service;

preservation storage model: a model of permanent storage;

preservation submitter: a legal or natural person (submitter, for example, a bank's client) using the preservation service to submit the data object;

preservation subscriber: a legal or natural person (client) bound by agreement with Evrotrust (for example, a bank, an insurance company, etc.);

proof of existence: a proof that a certain data object existed as of specific date / time**;**

proof of integrity: evidence that the data is protected and has not been altered;

EU qualified preservation service: a European qualified preservation service that meets the requirements for qualified preservation of qualified electronic signatures and/or qualified electronic seals as laid down in Regulation (EU) 910/2014;

signer: a creator of a signature;

submission data object: an original data object provided by the submitter;

time assertion: a time-stamp token or an evidence record;

time-stamp: a time-stamp representing data in an electronic form that binds other electronic data for a certain time establishing evidence that such data existed at that time;

time-stamping authority: a trust service authority issuing time-stamps;

time-stamping service: a service for issuing time-stamps;

time-stamping unit: a set of hardware and software which is managed as a unit and has a single time-stamp signing key;

rusted list: a trusted list providing information about the status and the status history of the trust services of trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation. In the context of the European Union Member States, as specified in Regulation (EU) No. 910/2014, it refers to a list of any qualified trust service providers from the EU member states, including information related to the qualified trust services rendered by them;

validation data: data used for validation of a digital signature.

preservation services with storage (WST) In this case, the data to be preserved is stored by the preservation service while the evidences and the preserved data are delivered upon request by the preservation service to the preservation client. The preservation service stores the submitted data object(s) (SubDO(s)) and the preservation object(s) (PO(s)) and the associated preservation evidences. The PO(s) are derived from the SubDo(s) by augmentation or by building a

Preservation Object Container (POC).

preservation services with temporary storage (WTS) The data to be preserved is stored temporary on the long-term preservation service side. The service temporary stores the submitted SubDO and the generated preservation evidence. Preservation evidence is produced synchronously after the SubDO is received. The preservation service keeps traces of its actions to be able to provide records of its activities.

1.7 ABBREVIATIONS

EDETSA – Electronic Document and Electronic Trust Services Act;

QTSP – Qualified trust service provider;

CSA (Certificate Status Authority) – Trust authority for status check (OCSP)

ER - Evidence Record

OVR - Overall

PO - Preservation Object

PDO - Preservation Data Object

PDS - Preservation of digital signatures

PGD - Preservation of general data

POC - Preservation Object Container

PRP - Preservation Service Protocol

PRS - Preservation service

PSP - Preservation Service Provider

QC - Qualified certificate

QES - Qualified electronic signature or qualified electronic seal

SubDO - Submission data object

SigS - Digital signature creation service

TS - Trust Service

TL - Trusted List

TSA - Time-Stamping Authority

TSP - Trust Service Provider

UTC - Coordinated Universal Time

ValS - Validation Service

WST - preservation service with storage

WTS - preservation services with temporary storage

2 RESPONSIBILITY FOR PUBLICATION AND STORAGE

Evrotrust publishes communication related to the company activity and all significant documents that might be of interest for the users and the relying parties at its website (https://www.evrotrust.com/).

Users and relying parties shall be informed about the Policy, Practice and General Terms of the qualified preservation service for qualified electronic signatures/seals before signing a contract. The documentation, including Policy and Practice, agreements, models, audit reports, etc. is published on the Evrotrust website immediately on each update. The operational certificates of the certifying authority are published immediately upon each issue of new certificates.

Evrotrust offers services related to access to the information stored in the repository, providing HTTP / HTTPS based access to it. The information published in the Evrotrust repository is permanently accessible (24/7/365), except in the cases of events beyond Evrotrust's control.

3 IDENTIFICATION AND CERTIFICATION OF IDENTITY

3.1 NAMES

The requirements applied by Evrotrust on the types of names are described in section 3.1 of the document "Practice of Qualified Certification Services ".

3.2 INITIAL VERIFICATION OF IDENTITY

Evrotrust verifies the identity of the sender and the recipient directly or through a third party:

a) remotely using means of electronic identification which is equivalent to the physical presence of the natural or legal person. The means of electronic identification meet the requirements referred to in Article 8 of Regulation (EU) No. 910/2014 with respect to the "significant" or "high" security levels.

For the purpose of customer identification, Evrotrust uses a remote video identification system via a mobile device that allows the provider to initially identify and remotely verify the identity of a person. In this system, the provider communicates with the national primary registers (civil registration, personal documents, corporation registers, etc.). After verification of the data provided, data are generated about the identity of the persons and they are stored in the Evrotrust for a period of 10 years in accordance with Art. 21 (3) of the Electronic Document and Electronic Certification Services Act.

b) when remote identification is not possible, Evrotrust allows the physical presence of the natural person, its authorize representative or the authorized representative of a legal person at an Evrotrust Registration Authority.

3.2.1 ESTABLISHING THE IDENTITY OF A NATURAL PERSON

The procedure is described in the document "Qualified Electronic Registered Delivery Service Policy and Practice" of "Evrotrust Technologies" AD".

3.2.2 ESTABLISHING THE IDENTITY OF A LEGAL PERSON

The procedure which Evrotrust applies to the initial verification of the identity of a legal person is described in the document "Qualified Electronic Registered Delivery Service Policy and Practice" of "Evrotrust Technologies" AD".

3.2.3 ESTABLISHMENT OF THE IDENTITY OF AN INDIVIDUAL WHO IS AN AUTHORISED REPRESENTATIVE OF A LEGAL ENTITY

The procedure which Evrotrust applies to the initial verification of the identity of a legal person is described in the document entitled "Qualified Electronic Registered Delivery Service Policy and Practice" of "Evrotrust Technologies" AD.

3.3 AUTHENTICATION OF A SENDER ON RE-USE OF SERVICE

The QPSES Evrotrust system allows sending user messages and attachments / files (user content) as shipment. No initial authentication is made, but only a validation of the identity of the data, when submitting a re-use request. The qualified preservation service customer is authenticated using cryptographic keys that he has received after successful identification in accordance with the established procedures described in Evrotrust's practice. In the process of service, the sender of electronic documents is authenticated and only then sends the shipment and has access to its contents.

4 SERVICE PROVISION PROCESS

4.1 REQUIREMENTS TO THE QUALIFIED PRESERVATION SERVICE FOR QUALIFIED ELECTRONIC SIGNATURES/SEALS

The QPSES service provided by Evrotrust meets all the requirements of ETSI EN 319 401, paragraph 6.1 as well as the requirements described of the document "Practice of Qualified Certification Services".

The QPSES service provided by Evrotrust meets the following specific requirements:

- Evrotrust supports service policy with OID: 1.3.6.1.4.1.47272.2.13;
- The preservation profiles that support the preservation service are described in paragraph 4.5;
- Realization of preservation targets (PDS and PGD) is described in point 4.2;
- The availability of SubDOs and related evidence is achieved through physical, informational and organizational security controls as described in this document;
- External organizations are not involved in the operation of Evrotrust when providing a storage service, but Evrotrust reserves the right to conclude contracts with outsiders for the provision of the service;
- The process of requesting incoming / outgoing packets includes receiving a written request from a user of the service or another person, which describes exactly which data is the subject of the request. Evrotrust processes the request, reserving the right to reject it without giving any reasons. If Evrotrust approves the request, the user / person receives the requested data in a securely protected electronic form;
- The input / output packets, the relevant storage evidence and the additional information required for their validation are accessed by using the service interface or by requesting a specific request for data and / or evidence. They can be provided separately or in an I/O package that is securely protected by encryption. In all cases, they are handed over only

to the client or his authorized representative;

- All QPSES provision information is stored for a period of 10 years in accordance with the national legislation of the Republic of Bulgaria (LEDEU). After the end of the period all available data is permanently destroyed, unless otherwise agreed;
- Evrotrust ensures authentication of the sender;
- Sending of data objects is secured by evidence stamped with electronic time stamp of Evrotrust in a way that excludes any possibility of unnoticed change in the data object;
- the availability, integrity and confidentiality of data objects is guaranteed by Evrotrust;
- the integrity of the data objects is protected when exchanged between the sender and the Evrotrust system;
- QPSES uses Qualified Time Stamps;
- To provide the service under this document, Evrotrust does not use external qualified certification service providers. Evrotrust reserves the right to conclude contracts with outside parties for the provision of certain certification services. (point 1.3.4)

4.2 FUNCTIONAL MODEL OF A QUALIFIED PRESERVATION SERVICE

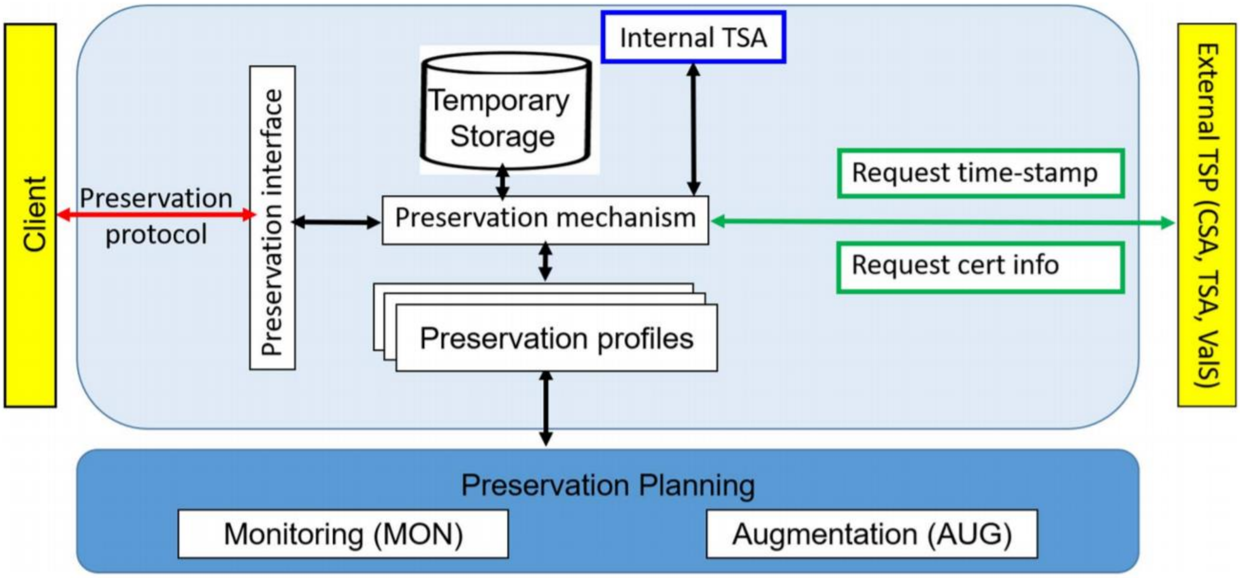


Figure 1: Long-term preservation service with temporary storage

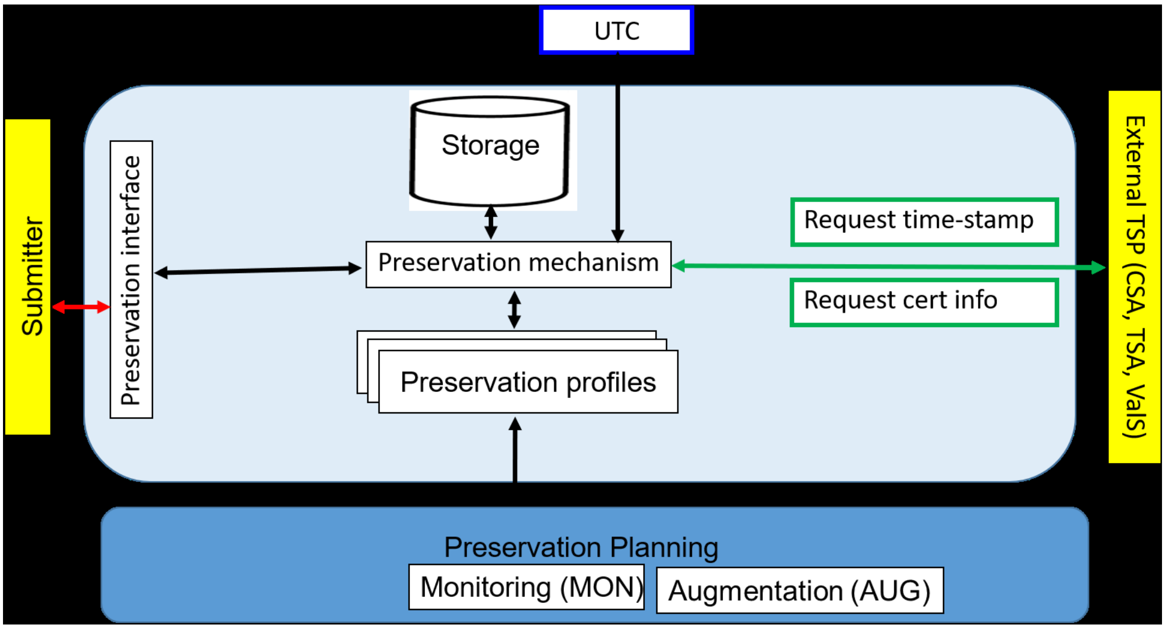


Figure 2: Long-term preservation service with storage

The Evrotrust QPSES CA is responsible for the qualified preservation of qualified electronic signatures/seals. "Evrotrust QPSES SU" with Object Identifier: 1.3.6.1.4.1.47272.2.13 as part of QPSES, signs the evidence to be given to the user when requested with a private key corresponding to a certificate issued by a certifying authority, which in this case is "Evrotrust Service CA" with OID: 1.3.6.1.4.1.47272.2.14 in the architecture of Evrotrust.

The protocol used ensures long-term preservation of digital signatures and general data using technologies of the digital signatures/seals and allow the submitter (e.g. a bank's client) of a preservation data object to interact with the preservation service interface.

The long-term preservation service with temporary storage (Figure 1) temporary preserves the information about the submitter/client together with the received data objects and the synchronously generates preservation evidence which is later retrieved by the client.

The long-term preservation service with storage (Figure 2) preserves the information about the submitter/client, as well as the preservation data objects received, through enhancing or building a preservation data object container and generating preservation evidence which it provides upon request. In such case the submitter provides the system with one or more preservation data objects, and the preservation service sends back a unique identifier of the preservation object. Then, during the preservation period, the submitter may extract upon request one or more preservation evidence and/or preservation objects. The qualified preservation service provides a possibility of deleting any preserved data objects. In case of deletion of preservation evidence, the respective subsystems also delete it but the preservation service preserves the preservation evidence till the end of the preservation period.

QPSES uses Evrotrust services, including the Certification Authority for the Issuance of Qualified Electronic Time Stamps, the Operations Certifying Authority and the Qualified Validation Authority.

The qualified preservation service uses a reliable time source (UTC) while creating preservation evidence. The time in the systems related to the service is synchronized with UTC at least once every 24 hours.

The qualified preservation service provided by Evrotrust to its customers (submitters/clients) uses secure and reliable cryptographic algorithms in the process of generation and extension of the reliability of any digital objects in the preserved evidence beyond their technological validity status.

Submitters access QPSES by using the interface specified in ETSI TS 119 512 Standard and by using the operations applicable to the specified profile.

The qualified preservation service provided by Evrotrust uses the electronic signature technology.

Evrotrust uses procedures and technologies to allow the reliability of qualified electronic signature to extend beyond the term of technology validity in order to extend the period of time, validate digital signatures and provide evidence of the availability of data for long periods of time. For extended duration of the validity status of electronic signatures/seals the qualified preservation service provides a proof of the existence of the signing, signed data and validation data. The preservation goals in the schemes used by Evrotrust are achieved by F2 and F3 schemes, profiles thereto and a Policy&Practice implemented in compliance with the requirements of ETSI TS 119 511 and ETSI TS 119 512 Standards.

Any data objects, the relevant preservation evidence and additional information necessary for their validation are accessed by using the interface of the service or by a specific request for provision of data and/or evidence. They may be provided separately or in an input-output package that is reliably protected by encryption. In any case they are handed over to the client or a representative authorized by him only. Evrotrust maintains information about all input-output packages prepared, including the event date and the criterion which the preserved objects included in the package were chosen by. The request compulsorily states the person requiring the data, the reasons for requiring it, as well as how he would like to receive it, for example, by electronic mail or on an electronic carrier. Evrotrust reserves the right to approve or refuse the execution of the request with no necessity to justify its refusal or to notify the requesting party of that, except in the cases determined by a normative act. For the purpose of providing the data and evidence Evrotrust may collect fees for ensuring the execution of the request filed.

Preservation evidence is created by using cryptographic algorithms and applicable cryptographic combinations in compliance with ETSI TS 119 312, including SHA-512. The specific formats of proofs are described and attached to each profile used.

If necessary, preservation evidence may be validated by using a qualified validation service in the meaning of Regulation (EU) 910/2014, if that is applicable to the respective evidence format. Evrotrust offers such a service and recommends its use.

If a user wants to obtain data objects and any preservation evidence related to them that are not currently available for a reason: archived data or other technological reason, he will be informed of the time interval in which the data will be available and since when it can be obtained.

4.2.1 EXPORT-IMPORT DATA PACKAGES

Evrotrust allows users of the preservation services to request export-import packages with stored data, evidence, and all the information needed to validate the evidence. Export-import packages can be used to move stored data from one preservation service to another preservation service. Evrotrust has used the export-import package format described in ETSI TS 119 512. The export-import packages use a standardized format. Export-import packages are provided only to an authorized legal or natural person.

Evrotrust stores records of all export-import packages provided, including the date of the event and the criteria that were used to select a set of preservation objects to be included in the export-import packages.

4.2.2 PRESERVATION OPERATIONAL PROTOCOLS

The communication channel between the preservation service user and QPSES is secured, i.e., Evrotrust ensures the security of user authentication and privacy. To this end, Evrotrust uses a protocol in accordance with the requirements of ETSI TS 119 512. The protocol used is protected against unauthorized use.

QPSES allows to retrieve information about current and pre-maintained preservation profiles as defined in ETSI TS 119 512.

QPSES allows one or more data objects (SubDOs) to be stored under a specific preservation profile by retrieving either a preservation object identifier or a proof of preservation (synchronous mode). The preservation object identifier can later be used to retrieve PO objects and / or to trace or delete POs or to update containers of preservation objects (asynchronous mode) as is defined in ETSI TS 119 512. QPSES allows to obtain traces of all operations associated with a particular preservation object identifier. QPSES allows you to search for specific preservation objects and retrieve a set of object identifiers that can be used in other operations. QPSES allows the evidence to be validated and a return report for its validation as defined in ETSI TS 119 512.

The Long-Term Preservation Service allows the retrieval of evidence and / or preservation objects (POs). POs may contain evidence (RetrievePO) as defined in ETSI TS 119 512. The service allows the deletion of the stored POs. If the evidence is deleted, the SubDO is also deleted. QPSES ensures that stored POs can only be deleted before the end of the preservation period when the deletion request is submitted along with appropriate justification. Each provided justification is recorded along with information about the request for deletion (DeletePO), as defined in ETSI TS 119 512. QPSES allows requires a set of object identifiers from data storage, which can be used to retrieve or delete POs. QPSES does not allow providing a new version of the already submitted POC (UpdatePOC), as defined in ETSI TS 119 512.

4.2.3 OPERATIONAL NOTIFICATION PROTOCOLS

QPSES does not define and does not provide a notification / notification protocol.

4.2.4 DATA AND EVIDENCE PRESERVATION PROCESS

A preservation service with temporary storage which stores the data to be preserved after the evidence has being created states the reasons for doing so in the Terms and conditions.

4.2.5 PRESERVATION EVIDENCES

The QPSES evidence includes a time-stamp token that conforms to IETF RFC3161 and the updated version RFC 5816. QPSES uses an electronic time stamp that matches the time-stamping protocol used, and the time-stamp token profile, as defined by ETSI EN 319 422.

QPSES records evidence in accordance with IETF RFC 4998 or IETF RFC 6283.

This policy is listed in the preservation profile, which makes it known to users of QPSES and third parties. Policy is cryptographically protected when included in the evidence.

4.2.6 PRESERVATION OF DIGITAL SIGNATURES

If the validation data is not submitted by the QPSES user, the preservation service makes its best efforts to collect and verify the validation data according to the signature validation policy supported by the preservation profile.

If the validation data is submitted by the QPSES user, the preservation service should verify the submitted validation data according to the signature validation policy supported by the preservation profile, and verify that the submitted validation data is appropriate, otherwise it should collect and verify the appropriate validation data.

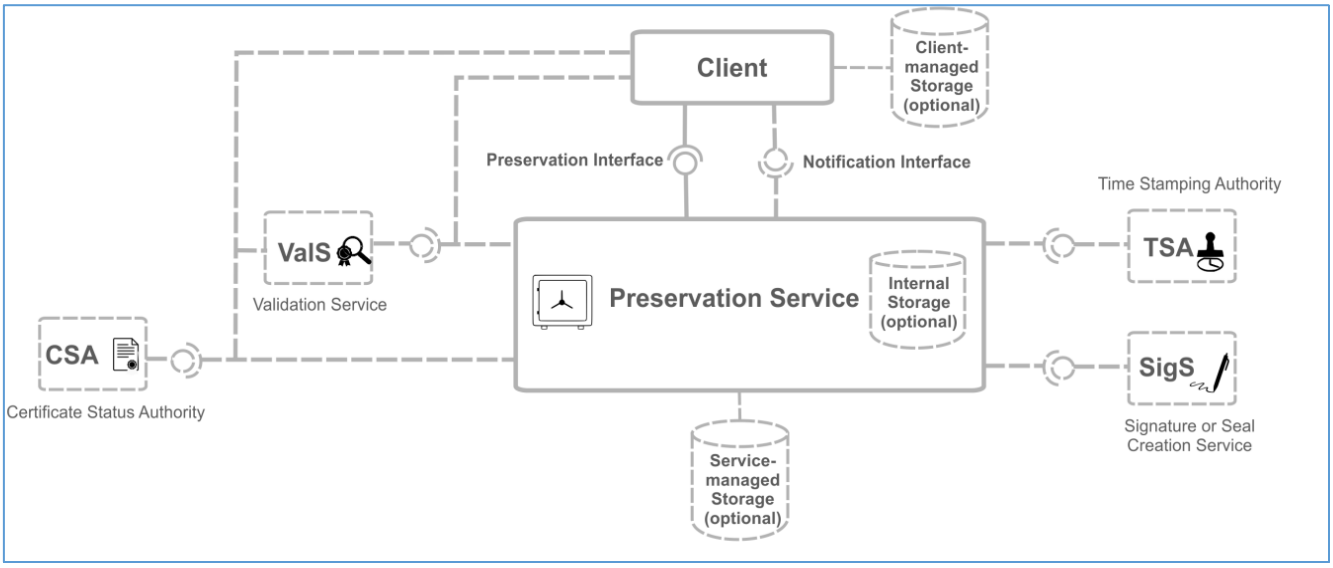
To extend the ability to validate a digital signature and to maintain its validity status, QPSES shall, at the minimum, provide a proof of existence of the signature and of the validation data needed to validate the signature using digital signature techniques (digital signatures, time-stamps, evidence records). A proof of existence of a detached signature provides also a proof of existence of the signed data at as long algorithms, e.g. the hash function used in the original signature is resistant against collision attacks.

To extend the ability to validate a digital signature and to maintain its validity status, QPSES, on one side, provide a proof of existence of the signature and of the validation data needed to validate the signature and on the other side a proof of existence of the signed data. The present document gives no restrictions on the way QPSES obtains the validation data needed to validate the signature.

In the case of a detached signature, the preservation service may allow the preservation subscriber to provide only a hash value of the signed data instead of the signed data itself. In case of a detached signature and if QPSES allows the preservation subscriber to provide only a hash value of the signed data, the PSP indicates in the preservation profile the identifiers of the hash functions that can be used. In case of a detached signature and if QPSES allows the preservation subscriber to provide only a hash value of the signed data, QPSES treats the hash value (associated with a hash function identifier) as a general data linked somehow to the signature, since it has no way of knowing if the hash value really corresponds to the signed data. In this case, QPSES is only responsible for the preservation of the submitted hash value (associated with a hash function identifier). In case of a detached signature and if the preservation service allows the preservation subscriber to provide only a hash value of the signed data, QPSES verifies that the submitted preservation object contains hash function identifiers that are in accordance with the identifiers of the hash functions listed in the preservation profile and that each hash value has a length in accordance with the associated hash function identifier.

The preservation service have one service digital identifier as defined in ETSI TS 119 612 which allows to uniquely and unambiguously identify the service within an trusted list.

4.3 SYSTEM ARCHITECTURE


Client
Client-managed Storage (optional)
Preservation Interface
Notification Interface
Time Stamping Authority
TSA
ValS
Validation Service
Preservation Service
Internal Storage (optional)
CSA
Certificate Status Authority
SigS
Signature or Seal Creation Service
Service-managed Storage (optional)

The qualified preservation service elaborated by Evrotrust provides interfaces for access to the system resources or external services. The qualified long-term preservation service uses its own storage under the control of Evrotrust. The service has the goal to preserve general data and ensure evidence of the data object submittal.

The period in which the qualified preservation service preserves the submitted data objects and any preservation evidence related to them by validation and enhancing of the qualified electronic signature reliability beyond the technological validity status or affixing a time stamp, is 10 (ten) years and then they are permanently deleted by the system.

In that period the qualified preservation service generates and extends the preservation evidence necessary for achieving the preservation goal. The method of creating evidence may change in that period in reasons, for example, the certificates expire or because the cryptographic algorithm is not reliable any more. Evrotrust keeps itself permanently informed by the ETSI standards (particularly TS 119 312) published on the European Commission's website in order to assess which cryptographic algorithms, key sizes or hash functions are probably not reliable any more, and if necessary, it issues a new preservation profile.

4.4 PRESERVATION SCHEMES

4.4.1 PRESERVATION SCHEME WITH TEMPORARY STORAGE BASED ON EVIDENCE RECORDS (F2[1])

- Unique identifier:
    - http://uri.etsi.org/19512/scheme/pgd+wts+ers;
- Preservation goal (general data):
    - Preservation of General Data (PGD);
- Preservation model (with temporary storage):
    - With temporary storage;
- List of operations supported by the preservation protocol:
    - PreservePO;
    - RetrievePO;
- Value specifying the time which the profile is deemed active from:
    - 01.01.2021;
- Supported formats for input:
    - Any files/data;

[1] *The scheme numbering complies with ETSI ES 119 512 Appendix F*

- Supported formats of preservation evidence:
  - Evidence Record according to IETF RFC 6283.

4.4.2 PRESERVATION SCHEME WITH ELECTRONIC SIGNATURE/SEAL AUGMENTATION AND WITH STORAGE (F3[2])

- Unique identifier:
  - http://uri.etsi.org/19512/scheme/pds+wst+aug
- Preservation goal (general data):
  - Preservation of Digital Signatures (PDS);
- Preservation model (with storage):
  - With storage;
- List of operations supported by the preservation protocol:
  - PreservePO;
  - RetrievePO;
  - DeletePO;
- Value specifying the time which the profile is deemed active from:
  - 01.01.2021;
- Supported formats for input:
  - CAdES digital signature according to ETSI EN 319 122;
  - XAdES digital signature according to ETSI EN 319 132;
  - PAdES digital signature according to ETSI EN 319 142;
- Supported formats of preservation evidence:
  - CAdES Archive Time Stamp V3 according to ETSI EN 319 122;
  - XAdES Archive Time Stamp according to ETSI EN 319 132;
  - PAdES Document Time-Stamp according to ETSI EN 319 142.

4.5 PRESERVATION PROFILES

A preservation profile identifies a set of implementation details specifying how

[2] *The scheme numbering complies with ETSI ES 119 512 Appendix F*

preservation evidence is generated and validated and which details are of significance for the preservation storage model and the preservation goal. A preservation scheme is a generic set of procedures and rules pertinent to a preservation storage model and one or more preservation goals which outline how preservation evidence is created and validated. Supported profiles are publicly available online. The type of account for the qualified preservation service is applied throughout the preservation period. The profile does not change over time. All the dynamic aspects are outlined in this policy. Evidence policy or signature validation policies listed in the account may change over time, but all versions of them associated with a particular account are publicly available, and for users it is clear which version and timing applies.

A qualified preservation service implements a qualified preservation service profile. A qualified preservation service profile is uniquely identifiable by URI.

A qualified preservation service profile specifies the following:

1. A unique identifier
2. A preservation storage model with storage
3. A preservation goal (digital signatures or general data)
4. List of operations supported by the preservation protocol
5. Value specifying the time which the profile is deemed active from
6. Supported formats for input
7. Supported formats of preservation evidence
8. Supported additional output formats, if any

Evrotrust supports the following digitally signed data objects for sending (SubDOwithDS):

- CAdES digital signature according to ETSI EN 319 122;
- XAdES digital signature according to ETSI EN 319 132;
- PAdES digital signature according to ETSI EN 319 142.

Evrotrust supports data objects for sending without electronic signatures (SubDOwoDS) which can be the very files/data or their hash sums calculated by SHA-512 algorithm. The exact list of supported types of data objects for sending without electronic signatures may be described additionally in the agreement with a client.

Size limitations that may also be described in the agreement with a client are applied to both types of data objects for submittal (SubDOwithDS and SubDOwoDS).

Evrotrust supports the following formats of preservation evidence:

- CAdES Archive Time Stamp V3 according to ETSI EN 319 122;
- XAdES Archive Time Stamp according to ETSI EN 319 132;
- PAdES Document Time-Stamp according to ETSI EN 319 142;
- Evidence Record according to IETF RFC 6283.

Evrotrust does not support any additional formats of preservation containers (PO).

4.5.1 PRESERVATION PROFILE F2.1

The qualified preservation service profile F2.1 complies with scheme F2 described above:

1. Unique identifier:
    - http://www.evrotrust.com/PreservationService/ProfileF2.1;
2. Description:
    - PGD withTemporarytStorageBasedOnEvidenceRecords for AnyFiles
3. Preservation goal (general data):
    - Preservation of General Data (PGD);
4. Preservation model (with temporary storage):
    - WithTemporaryStorage
5. Maximum volume:
    - 100 MB unless the agreement with the client describes otherwise;
6. List of operations supported by the preservation protocol:
    - PreservePO;
    - RetrievePO;
7. Value specifying the time which the profile is deemed active from:
    - ValidFrom=01.01.2021,
8. The service supports formats for input:

- Any files/data;

9. The service supports formats of preservation evidence:
   - Evidence Record according to IETF RFC 6283,
10. No additional output formats are supported.
11. Applicable technical policies:
    - PreservationEvidenceCreationPolicy: urn: oid: 1.3.6.1.4.1.47272.2.13;
    - PreservationEvidenceValidationPolicy: urn: oid: 1.3.6.1.4.1.47272.2.9.
12. Preservation evidence retention period:
    - At least 5 minutes.
13. Expected evidence duration (based on ETSI TS 119 312 requirements):
    - At least 30 days.

4.5.2 PRESERVATION PROFILE F2.2

The qualified preservation service profile F2.2 complies with scheme F2 described above:

1. Unique identifier:
   - http://www.evrotrust.com/PreservationService/ProfileF2.2
2. Description:
   - PGD withTemporarytStorageBasedOnEvidenceRecords for SHA-512
3. Preservation goal (general data):
   - Preservation of General Data (PGD);
4. Preservation model (with temporary storage):
   - WithTemporaryStorage;
5. Maximum volume:
   - 64 bytes;
6. List of operations supported by the preservation protocol:
   - PreservePO;
   - RetrievePO;
7. Value specifying the time which the profile is deemed active from:
   - ValidFrom=01.01.2021,
8. The service supports formats for input:

- SHA-512 hash of documents/files;

9. The service supports formats of preservation evidence:
   - Evidence Record according to IETF RFC 6283,
10. No additional output formats are supported.
11. Applicable technical policies:
    - PreservationEvidenceCreationPolicy: urn: oid: 1.3.6.1.4.1.47272.2.13;
    - PreservationEvidenceValidationPolicy: urn: oid: 1.3.6.1.4.1.47272.2.9.
12. Preservation evidence retention period:
    - At least 5 minutes.
13. Expected evidence duration (based on ETSI TS 119 312 requirements):
    - At least 30 days.

4.5.3 PRESERVATION PROFILE F3.1

The qualified preservation service profile F3.1 complies with scheme F3 described above:

1. Unique identifier:
   - http://www.evrotrust.com/PreservationService/ProfileF3.1
2. Description:
   - PDS with signature augmentation and with storage
3. Preservation goal (electronically signed data):
   - Preservation of Digital Signatures (PDS)
4. Preservation model (with storage):
   - WithStorage
5. List of operations supported by the preservation protocol:
   - PreservePO;
   - RetrievePO;
   - DeletePO;
6. Value specifying the time which the profile is deemed active from:
   - ValidFrom=01.01.2021,
7. The service supports formats for input:
   - CAdES digital signature according to ETSI EN 319 122;

- XAdES digital signature according to ETSI EN 319 132;
- PAdES digital signature according to ETSI EN 319 142;

8. The service supports formats of preservation evidence:
    - CAdES Archive Time Stamp V3 according to ETSI EN 319 122;
    - XAdES Archive Time Stamp according to ETSI EN 319 132;
    - PAdES Document Time-Stamp according to ETSI EN 319 142;
9. No additional output formats are supported;
10. The evidence preservation period is 10 years, unless the agreement with the client states otherwise or there is another period determined by a normative act.
11. Applicable technical policies:
    - PreservationEvidenceCreationPolicy: urn: oid: 1.3.6.1.4.1.47272.2.13;
    - PreservationEvidenceValidationPolicy: urn: oid: 1.3.6.1.4.1.47272.2.9.

4.6 EVIDENCE PRESERVATION POLICY REQUIREMENTS

The evidence preservation policy fulfils the following requirements:

- The evidence preservation policy that is specified by the qualified preservation service account is described with its Object Identifier (OID);
- 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.;
- The policy contains a description of the way in which the evidence is created (4.9), including which cryptographic algorithms are used (6.2.1);
- The cryptographic algorithms used are in accordance with the recommendations of TS 119 312 (6.2.1);
- Evidence preservation policy includes a description of all participants in the Evrotrust infrastructure that are part of the qualified preservation service for qualified electronic signatures/seals, including the Certification authority for the Issuance of Qualified Electronic Time Stamps, the Operational Certifying Authority and the Qualified Validation Authority (item 1.3, item 7 and item 6.8);
- The evidence preservation policy describes how the evidence of storage is validated

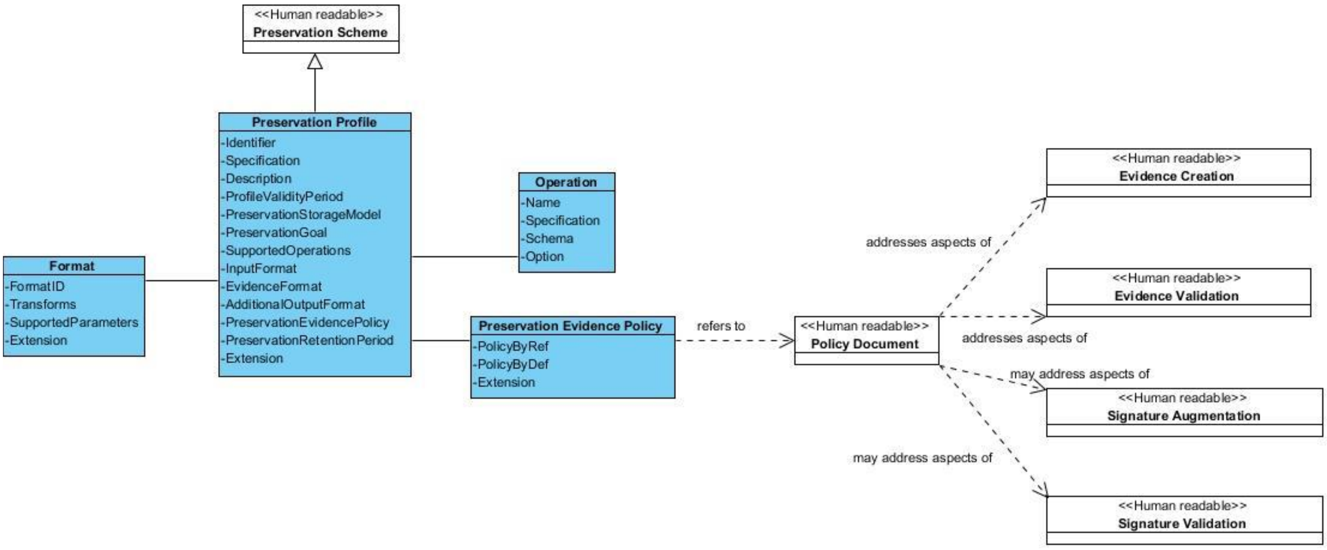
(clauses 4.2, 4.2.6 and 4.7);

- The policy indicates how the validity of the evidence is extended (point 4.9);
- Policy describes the form of evidence of storage (item 4.9).

4.7 SIGNATURE VALIDATION POLICY

The signature validation policy is contained in the presesrvation profile and is described by its object identifier (OID: 1.3.6.1.4.1.47272.2.9).

4.8 RELATION BETWEEN THE SCHEME, THE SUPPORTED PRESERVATION PROFILE AND THE POLICY&PRACTICE



A qualified preservation service supports a preservation profile. Technically, the profile allows the submitter to use the interface and communicate with the qualified preservation service. The profiles are related to the policies of evidence generation and validation, as well as the signature augmentation and validation. A preservation profile references a preservation scheme for the specifications of general rules. A preservation scheme is a generic set of procedures and rules pertinent to a preservation storage model and the preservation goals, which outline how preservation evidence is created and validated. A preservation profile has an identifier that identifies it uniquely.

4.9 COLLECTION OF EVIDENCE

When collecting and storing the evidence, the requirements of ETSI EN 319 401, clause 7.10, applies as follows:

- ➢ QPSES collects and keeps registration files of the events in order to have information necessary for later evidence;
- ➢ Evrotrust records and maintains accessible for a reasonable period of time (including after its business termination) all the information regarding data issued and received during QPSES provision to be used, if necessary, in court proceedings and for ensuring a continuous service;
- ➢ The period of preservation of the collected evidence is in accordance with national legislation and is 10 (ten) years, and is in line with the recommendations of ETSI TS 119 312;
- ➢ The confidentiality and integrity of the current and archived records regarding the operation of the service are preserved and archived in accordance with the business practice of Evrotrust;
- ➢ The time used for recording events as required in the registration log is synchronized with UTC at least once a day;
- ➢ Events are recorded in a manner that may not be deleted or destroyed easily;
- ➢ The same preservation profile for the qualified preservation service is applied throughout the period of evidence preservation;
- ➢ The validity period of the evidence is expanded using secure and reliable cryptographic algorithms;
- ➢ The format of the evidence under this policy follows the requirements of IETF RFC 6283 as well as CAdES ETSI EN 319 122, XAdES ETSI EN 319 132 and PAdES ETSI EN 319 142.

Where necessary, QPSES extend the validity of preservation evidence. During the preservation period, the preservation service checks that the evidence can be used to achieve the appropriate conservation purpose. This can be threatened if the cryptographic algorithm can no longer be trusted or more cannot be obtained for termination of the certificate. In such cases, QPSES complements / expands the evidence before it cannot be used to achieve the appropriate preservation purpose to ensure that the preservation purpose is met.

4.10 PROTECTION OF STORAGE DATA AGAINST THE RISK OF LOSS, THEFT, DAMAGES OR UNAUTHORIZED AMENDMENTS

All carriers containing software, data archives or audit information are safely preserved in a special archive premise with implemented control of access. Evrotrust's archive premise has a system of physical and logical protection.

Confidentiality and integrity of data are important to the operation of Evrotrust and therefore cryptographic data protection techniques on removable media are used. For mitigation of the risk of carrier obsolescence, while the preserved data is still necessary, the data is transferred onto new media before they become illegible. Evrotrust preserved multiple copies of valuable data on different media to further reduce the risk of accidental damage or loss of data.

Evidence is reliably stored by subsequent loss and theft in a protected environment under the control of Evrotrust for 10 (ten) years.

4.11 END OF THE SERVICE SUBSCRIPTION

Upon termination of the contract for the provision of a qualified preservation service between Evrotrust and user / customer, the service subscription is terminated. The contract for certification services between Evrotrust and user / customer is terminated in accordance with the termination clauses entered into it. Upon termination of a contract, Evrotrust will stop access to the service in a timely manner. All user / client documents and evidence related to the performance of the service shall be retained until the expiry of the statutory period, unless otherwise agreed in the contract.

4.12 TRUST PRESERVATION OF PRIVATE KEYS (ESCROW)

The private keys of the Evrotrust certification authorities and users who have requested remote service usage through the Evrotrust mobile application are subject to trusted preservation service of Evrotrust (ESCROW) and are stored in a hardware security module (HSM) encrypted, certified for FIPS 140-2 Level 3 security level.

5 CONTROL OF PHYSICAL AND ORGANIZATIONAL SECURITY

5.1 PHYSICAL SECURITY CONTROLS

The system physical security meets the requirements of international standards and recommendations. The protection of the Evrotrust building is realized by 24-hour security. Strict control is applied for preventing company asset loss, damage or compromise, suspension of activities, as well as for avoiding compromise or theft of information and information processing equipment.

An alarm system, a surveillance system, a fire alarm system and an access control system are installed in Evrotrust's premises.

The offices of the Registration authorities are detached from the rest of the premises at Evrotrust. They are equipped with devices allowing safe data and document preservation the access to all areas is monitored and restricted to authorized persons in compliance with their activity.

Evrotrust's buildings have installations for power supply and ventilation, protection against floods and fire.

5.1.1 PREMISES AND CONSTRUCTION OF ROOMS

Evrotrust has a specially designed and equipped room with the highest degree of physical access control, housing the certifying authorities and all the central components of the infrastructure.

5.1.2 PHYSICAL ACCESS

The physical security of the systems is in line with the requirements of international standards and recommendations. For the equipment in the secure and isolated room of Evrotrust, physical integrity is ensured. There is two-factor access control and 24-hour armed physical security. Physical access to critical equipment is not allowed for more than 30 (thirty) minutes per visit. No access to the commode with the equipment of less than 2 (two) authorized persons of Evrotrust is allowed. Every access to critical infrastructure premises is documented in special journals.

5.1.3 ACCESS CONTROL

The access to Evrotrust's system is limited to authorized persons:

- controls (for example, firewalls) protect Evrotrust's internal network domains from unauthorized access, including access of clients and third parties;
- firewalls are configured to stop all protocols and ensure access to Evrotrust's activities only.
- The access to the information and functions of the system applications is limited as per the policy of access control;
- The provider grants administrator's access to the operators, administrators and system auditors. The management controls the users' accounts, timely change or access removal.
- The access to the information and system is limited in compliance with division of the trusted roles;
- Evrotrust's employees identify and certify themselves prior to using critical applications related to the service;

Evrotrust has undertaken measures to protect the company sensitive data against disclosure and unauthorized access. Evrotrust's employees are responsible to the management for non-fulfilment of their obligations.

5.2 INFORMATION SECURITY

Evrotrust has an information security policy approved by the management and determining the company approach to its information security management. Changes in the information security policy are communicated to any third parties where applicable. The information process includes submitters, clients, trusting parties, assessment authorities, supervising or any other regulatory authorities.

The provider has undertaken all necessary security measures to preserve the data object integrity and confidentiality. QPSES guarantees that the data object availability, integrity and confidentiality are protected from the submittal to the receipt in Evrotrust's system, including during the transmitting of the contents among its system components.

Evrotrust's information security policy is documented, regularly updated and strictly implemented, including the security controls and the business operational procedures, the provider's systems and information assets rendering the services. The maximum interval between two inspections is 1 (one) year.

Evrotrust undertakes the responsibility for the compliance of its business with the procedures specified in its Information security policy, even where certain activities are performed by hired contractors. Evrotrust determines the responsibility of any hired contractors and ensures that all necessary controls for secure and reliable work have been implemented in their activity.

Evrotrust's information security policy and any risks, threats and vulnerabilities in the asset risk assessment are reviewed and updated in planned intervals or if significant changes occur in order to guarantee their continuous fitness, adequacy and effectiveness. Any changes that would affect the level of security provided are approved by the management. The provider's system configuration is checked regularly for changes that would infringe Evrotrust's security rules. The maximum interval between two inspections is 1 (one) year.

Evrotrust uses exclusively reliable systems and products protected from modification and guarantee the technical security and reliability of the processes maintained by them. All hardware changes are monitored and registered by authorized employees of Evrotrust. Where new technical equipment is purchased, it is delivered with the required operation procedures and instructions for use.

Supervision over the technological system functionality is carried out and it is guaranteed that it operates properly and as per the delivered production configuration. Procedures of control of changes are applied in case of changes in the configuration. The integrity of the systems and any information about the provider are protected against viruses, malicious and unauthorized software. The procedures of records management ensure protection against obsolescence and aggravation within the preservation period.

5.2.1 INCIDENT MANAGEMENT

Evrotrust classifies security incidents in two categories:

- Such jeopardizing the trust service integrity (for example, penetration or change in the location of a data object/data package, errors in maintaining the system jeopardizing the integrity of the systems/servers, physical access of unauthorized persons);
- Such, not jeopardizing the trust service integrity (for example, loss of power supply,

damage on the communication lines, misuse of authorities, attempts of penetration in the system).

In case of doubt which category a security incident is classified in, it is deemed classified of the highest degree.

Evrotrust performs monitoring over the sensitivity of any collected information and analyses it. Abnormal system activities showing potential security infringement, including penetration in the network, are detected and reported as alarms. The start and the end of the registration functions are monitored, as well as the service availability and use with Evrotrust's network.

Evrotrust has employed trusted personnel monitoring the signals about events of potentially critical security and guarantees that all incidents are communicated as per the company procedures. The procedures for reporting and responding in case of incidents are applied in a manner minimizing the damages from security incidents. Any person seeing or suspecting a security incident has the obligation to inform the management. Reporting security incidents is performed in any manner (personally, by phone, IMS or email) allowing the fastest notification of the relevant managers.

The management is obliged to investigate the reported incident and undertake or propose appropriate measures for avoiding another similar incident. Every security incident is recorded in a protocol. Evrotrust establishes procedures of notifying the relevant parties concerned as per the applicable regulatory rules for each security infringement or loss of inviolability, which significantly affects the trust of the trust service provided and any personal data maintained in it within 24 hours from the breach identification. Where security infringement or loss of data may have an unfavourable impact on a natural or legal person using the service, the provider notifies the person of the incident.

Evrotrust considers each critical vulnerability within 48 hours from its finding.

5.3 STAFF CONTROL

Evrotrust guarantees that employees perform administrative and management procedures and procedures which are in compliance with the information security management and thus ensure reliability and security of its business. Evrotrust employs personnel and, if applicable, subcontractors having the necessary experience, reliability and qualification and who have undergone training on the security and protection of personal data. Evrotrust applies appropriate disciplinary sanctions to employees who infringe the company policies or procedures.

The roles and responsibilities for information security are recorded in the job descriptions of the personnel. Duties and responsibilities are segregated and careful not to have a conflict of interest in order to reduce the possibilities for unlawful or unintentional misuse of Evrotrust assets. The company management holds the necessary experience and knowledge about the provided QPSES service and they are aware of the procedures of security and risk assessment sufficient for performing managerial functions.

None of the provider's personnel has a conflict of interests that could infringe Evrotrust's impartial business.

All procedures concerning the security at providing QPSES are performed by trust personnel of Evrotrust employed on a contract on the principle of the least privilege of access or at configuring privileges of access. The personnel has no access to trusted functions until the necessary checks have been completed (including obtaining information of clear criminal records). Employees with trusted roles are checked prior to their employment to have no conflict of interests that could infringe Evrotrust's impartial business.

Evrotrust maintains a sufficient number of qualified employees to ensure compliance with the applicable legislation and the company in-house rules at any time of carrying on its business. The functions are distributed so that the risk of compromising, leak of confidential information or occurrence of conflict of interests is minimized as much as possible.

Evrotrust has employees performing the following trusted roles:

a). security administrator: overall responsibility for the management and performance of the system security procedures: he elaborates a security policy; he undertakes measures of technical protection of data and systems; he determines the operational security measures; he carries out direct control over the compliance with the security requirements for information systems monitoring the compliance with the security procedures during installation, configuration, maintenance and modifications in the information systems or network;

b). system administrator: he is responsible for installation, configuration and maintenance of reliable service management systems; system recovery if necessary; re-configuration of devices and systems for implementation of new services or solutions; monitoring the technical and software status of the servers and notification of failures;

c). system operator: he is directly responsible for the operation of Evrotrust's reliable technological systems and for the creation of a system backup: creation and management of certificates for a qualified electronic signature/seal, including the creation of a pair of key certificates, private and public for a qualified electronic signature/seal; use of efficient technologies for ensuring the system's everyday work; carrying on tests and verifications for the system's trouble-free work and security; following any technical requirements for device operation and notification of the responsible officials in case of established technical failure;

d). system auditor: data preservation, archiving and management of the event registers (in particular, for checking their integrity) at performing in-house inspections; responsibility for the effectiveness of the internal audit; for the verification of compliance with Regulation (EU) No. 910/2014; responsibility for the activity of all registration authorities working within Evrotrust.

The procedures applied by Evrotrust on staff control are described in the document "Qualified Electronic Registered Delivery Service Policy and Practice ".

5.4 AUDIT PROCEDURE

The reviews (audits) performed in Evrotrust concern the processing of information data and the management of key procedures. Evrotrust annually performs at least one internal audit. The provider has successfully undergone an audit from an external company and is certified under the following ISO standards: ISO 9001, ISO 22301, ISO/IEC 27001 and ISO/IEC 20000-1. The subjects of activity examined during the audits for each of the standards are as follows:

➢ ISO 9001, ISO 22301- Provision of services related to electronic identification and services under Regulation (EC) No. 910/2014;

➢ ISO/IEC 27001– Information Security Management System for processing of personal data of customers, corporate data and information systems for the provision of electronic identification and certification services in accordance with the Declaration of Feasibility version 1.0.;

➢ ISO/IEC 20000-1 - IT Service Management System for the provision of services related to electronic identification and certification services to external customers in accordance with a catalogue of services.

Evrotrust is audited at least once every 24 months by a Conformity Assessment Body. The purpose of the audit is to confirm that the Qualified Trust Service Provider (QTSP) and the certification services provided by it meet the requirements according to Regulation (EU) No. 910/2014.

The internal and external audit reports are delivered to the Evrotrust management.

The report by the Conformity Assessment Body is delivered to the Supervisory Authority within 3 (three) days of its service to the Evrotrust management. The Supervisory Authority will examine the report and decide on whether to leave or revoke the qualified status of the provider.

On the basis of the assessments made from the reports, the Evrotrust management will set out measures and deadlines for remedying any identified deficiencies and inconsistencies.

5.5 ARCHIVING

The arvhiving procedure is described in Section 5.5 of the "Qualified Certification Services Practice" document.

The information under Art. Article 24 (2) (h) of Regulation (EU) No 910/2014 (all relevant information in relation to data issued and received by EVrotrust, in particular with a view to providing evidence in court proceedings and insurance of continuity in the provision of the service) is stored for a period of 10 years, including after the termination of the activity of EVrotrust. The long-term preservation of data is done in a secure and protected premise. The specific conditions are in line with the applicable standards, recommendations and regulations specified in the field of information security. Data is collected in a way consistent with the type of document. Access to the long-term stored data is only allowed to authorized persons.

5.5.1 STORAGE OF DATA MEDIA

The procedure is described in the paragraph 5.1.6 of the document entitled "Practice of Qualified Certification Services".

5.5.2 WASTE DISPOSAL

The procedure is described in the paragraph 5.1.7 of the document entitled "Practice of Qualified Certification Services".

5.5.3 ASSET MANAGEMENT AND RISK ASSESSMENT

Evrotrust provides an adequate level of protection for its assets, including information assets. Provider Evrotrust maintains a list of all information assets and makes a risk assessment. Evrotrust makes a risk assessment to identify, analyse and assess the risks associated with the certification service, business, and technical issues. The TSP shall choose appropriate risk management measures considering the results of the risk assessment. Risk management measures ensure that the level of security is commensurate with the degree of risk. Procedures for managing information security risk are part of the security management system. Evrotrus meets all the security requirements and operational procedures that are required to implement the risk management measures as documented in the Information Security Policy and this document. Risk assessment is reviewed regularly. The Evrotrust management approves the risk assessment and accepts the residual risk.

Evrotrust identifies the assets corresponding to the information life cycle and documents them by their significance. The information life cycle includes creation, processing, preservation, exchange/submittal, deletion and destruction. The documentation is kept in special lists. The list of assets is precise, updated and consistent.

Information is classified according to the requirements of the normative acts, its value, criticality and sensitivity to unauthorized disclosure or modification. Documentation containing sensitive data is destroyed safely when not required any more. Asset operation procedures have been elaborated in compliance with the information classification scheme adopted by Evrotrust.

5.5.4 RECORDS OF EVENTS AND MAINTENANCE OF JOURNALS

Evrotrust keeps records of:

➢ events related to the initial verification of the recipient's identity and/or additional authentication. The records contain a description of the documents submitted by the person who wishes to be identified (e.g. ID document, power of attorney, etc.) as well as data relating to unique identification data, numbers or a combination thereof or copies of applications and identity documents, including a signed contract, an agreement with the Evrotrust Policy and Practice, and the provision of personal data and etc.

- ➢ events related to the sending and receipt of user content;
- ➢ security events, including security policy changes, system start up and shutdown, system failures and hardware failures, firewall and router and attempts to access the PKI system;
- ➢ the records related to the operation of the QERDS service are reliably and confidentially archived in accordance with the company's business practices;
- ➢ the exact time of significant events of key management and clock synchronization. The system time is synchronized against UTC at least once every 24 hours;
- ➢ events are recorded in a way that does not allow for them to be easily deleted or destroyed;
- ➢ events having a significant impact on the security and reliability of the technology system, staff and customer control and impact on the security of the QERDS provided are recorded.

Collected documents relating to the provision of the service are provided as evidence, for example, for the purpose of court proceedings.

Evrotrust ensures the privacy, integrity, and availability of the journals.

The information about the electronic journals is generated automatically. Journals of records of registered events are stored in files for at least 6 (six) months. Throughout this period of time they are available online or in the process of searching by an authorized Evrotrust employee. After this period, the records are archived. Archived journals are kept for a period of 10 (ten) years. An archive is signed with an advanced electronic signature and qualified electronic time stamp. The log record information is periodically recorded on physical media stored in a special safe located in a premise with a high degree of physical protection and access control.

5.6 CRYPTOGRAPHIC CONTROLS

Evrotrust applies the requirements set out in paragraph 7.5 of ETSI EN 319 401 described in the document "Practice of Qualified Certification Services".

In addition, Evrotrust applies the following key management requirements for the keys used to generate and validate the evidence:

➢ Evrotrust ensures that time storages used in the preservation process come from the Time Certification Authority ("Evrotrust TSA") that meets the requirements of state-of-the-art security practices and policies for the issue of qualified time stamps. The activity of "Evrotrust TSA" complies with the requirements of ETSI EN 319 421;

➢ Evrotrust uses qualified time stamps that are electronically signed with qualified certificates for qualified electronic stamps that can be checked using CRLs or OCSPs in the preservation process. In case of termination of the public key certificate that has signed the time certificate, the CRL or OCSP responses contain a "reason code";

➢ "Evrotrust QPSES SU" signs the evidence with a certificate issued by a trusted CA, in this case "Evrotrust Service CA", which fulfils the requirements of ETSI EN 319 411-1 and ETSI EN 319 411-2;

➢ The private signing key of "Evrotrust QPSES SU" is kept and used in a cryptographic module that:

a) is a reliable system that has an EAL 4 security level or higher in accordance with ISO / IEC 15408 or equivalent national or internationally recognized IT security assessment criteria. This refers to the security objectives or security profile that meets the requirements of this document based on risk analysis and taking into account physical and other non-technical security measures; or

b) meets the requirements set out in ISO / IEC 19790 or FIPS PUB 140-2, level 3;

➢ The cryptographic device in which Evrotrust QPSES SU private key is stored is protected and meets the requirements of the above section of this document;

➢ All backup copies of the Evrotrust QPSES SU private key for signing evidence are securely protected in case of storage outside the cryptographic module (HSM) to ensure their integrity and confidentiality.

Evrotrust performs cryptographic monitoring. For each supported storage profile, Evrotrust monitors the strength of each cryptographic algorithm used in connection with this account. In the event that one of the algorithms or parameters used is considered to be less certain or the validity of the relevant certificate expires or is updated by the relevant evidence policy or a new preservation profile is created to deal with newly released data objects.

If any of the algorithms or parameters used in the proof of storage is less secure or the validity of the relevant certificate expires, QPSES will extend the validity of the proof of storage in accordance with a new version of the storing policy.

The cryptographic algorithms used to provide a qualified storage service to qualified electronic signatures / stamps meet the requirements set forth in ETSI TS 119 312. The applicable combinations of asymmetric and hash algorithms with respect to the security of the qualified electronic signature over time is as specified in ETSI TS 119 312. The length of the key that meets the requirements of ETSI TS 119 312 is used.

5.7 CHANGE OF KEYS

The Provider may change the Keys of the Certification authority "Evrotrust Services CA" and the Signatory „Evrotrust QPSES SU“, in the case of:

- expiration of the validity of the accompanying certificate;
- Changes in security key privacy attributes and requirement for new applicable cryptographic combinations and algorithms;
- in case of suspicion of compromise.

Upon change of the private keys in Evrotrust, the following rules are observed:

- "Evrotrust QPSES SU“, whose key is the signature of the evidence, and whose key will be changed, suspends the issuance of certificates 60 (sixty) days before the remaining period of validity of the private key is equal to the period of validity of the last signed proof;
- The "Evrotrust Services CA" Certification Authority, whose private key signs the „Evrotrust QPSES SU“, Certificate and the CRL and whose private key will be changed, continues to publish lists signed with the old private key to the moment when the last signed certificate expires.

5.8 COMPROMISE AND RECONSTRUCTION IN DISASTERS

The procedures followed by Evrotrust for disaster compromise and reconstruction are described in the document "Practice of Qualified Certification Services".

Evrotrust has developed procedures to manage the continuity of its operations. In case of service interruptions, it strives to minimize these interruptions so as not to affect customer / customer activity.

5.8.1 MANAGEMENT AND CONTINUITY PLAN

Evrotrust has created and maintains a continuity plan in case of disaster. In case of disaster, including compromising of a private signing key, operations are resumed within the delay established in the continuity plan. The causes of the disaster are considered and reasonable measures are determined for removing the cause of the process interruption, as well as measures to prevent such disasters in future.

The company has created, documented, implemented and maintained plans, procedures and control mechanisms in compliance with the international standard ISO 22301 to ensure the necessary level of business continuity and information security continuity during unfavourable cases.

Evrotrust ensures:

a) an available adequate management structure in order to prepare itself, mitigate and respond to a destructive event using personnel with the necessary authorities, experience and competence;

b) elaboration and approval of plans and procedures for response and recovery describing in detail how the company will manage a destructive event and maintain the continuity of information security;

c) mechanisms of control of the information security within the procedures and maintaining systems and instruments for business continuity and recovery after a disaster;

d) compensating mechanisms of control of the mechanisms of control of the information security which cannot be maintained in an unfavourable case.

The continuity plan includes backing up of the critical systems. Backup is stored at geographically remote places. The particular conditions comply with the applicable standards, recommendations and regulations stated in the area of information security. The company checks any created control mechanisms of the continuity of the information security at regular time intervals, so it can ensure their effect and efficiency in unfavourable cases. Evrotrust makes regular backups of important information and software and guarantees that all basic information and software may be recovered after a disaster or in case of loss of the archive.The recovery mechanisms are checked regularly, so it can be guaranteed that they meet the requirements of the work continuity plan.

The provider's database necessary for the recovery of the activity on QPSES in case of an incident or a disaster is maintained and stored at safe and secure places. Evrotrust has the obligation to inform the submitters, subscribers and any third parties of incidents occurred in the activity of providing the service.

5.9 TERMINATION OF THE ACTIVITY OF A CERTIFYING AUTHORITY

Before the certifying authority "Evrotrust Services CA" terminates its services, Evrotrust does the following:

- follows an updated and approved by the management plan and a scenario for the termination of the activity of a certifying authority. Information may be provided by email or by posting;
- informs customers, the Supervisory Authority and third parties about the termination of the activity of its certifying authority. Information is provided by email or by posting on the Evrotrust website;
- terminates the authorization of all persons having contract activities to carry out activities related to the particular certifying authority;
- before termination of the activity of the certifying authority, within a reasonable time, transfers its obligations for maintenance of all the information which is necessary to provide evidence to a trustworthy party;
- before termination of the activity, private keys, including backups, are destroyed or removed from use in such a way that personal keys cannot be retrieved;
- if possible, transfer its activity to another qualified provider;
- Evrotrust applies measures to cover costs in the event of bankruptcy or for other reasons for terminating the activity of a certifying authority. In the event that it is unable to cover the costs itself, it has provided for measures within the framework of the applicable

legislation;

- changes the status of the operating certificate;
- terminates the issuance of new certificates, but continues to manage the active certificates until the end of their validity;
- makes reasonable commercial efforts to minimize distortion of consumer interests.

Evrotrust monitors and prevents the issuance of a certificate for a period longer than the validity of the certifying authority that issued it.

5.10 TERMINATION OF EVROTRUST'S BUSINESS

Prior to the termination of its services the certificating authority has the obligation to:

- notify the Supervision authority of its intention to terminate its services in case of a claim the company to be adjudged bankrupt, the company to be declared invalid or of another request for termination or of the initiation of liquidation proceedings. The notification should be made 4 (four) months prior to the agreed termination date;
- notify (at least 4 months in advance) its clients of the decision to terminate the services rendered by him;
- change the status of its certificates;
- terminate all users' certificates within the period declared for termination of the business;
- make reasonable business efforts for minimizing the infringement of the clients' interests;
- perform the necessary actions for the Supervision authority to maintain the List of suspended and terminated certificates (CRL).

If a Registration authority, as an external organization, has decided to terminate Evrotrust's representation regards provided trust services, it is obliged to:

- notify Evrotrust of its intention to terminate the business. The notification should be served 1 (one) month prior to the agreed termination date;
- hand over to Evrotrust all the documentation related to the users' service, including the archive and audit data.

5.10.1 TRANSFER OF BUSINESS TO ANOTHER QUALIFIED TRUST SERVICE PROVIDER

In order to ensure continuity of a qualified preservation service Evrotrust may sign an agreement with another qualified trust service provider. In such case Evrotrust:

- notifies the Supervision authority of its intention not later than 4 months prior to the date of termination and transfer of the business;
- makes all efforts and takes care the service to be continued;
- notifies the Supervision authority and the clients in writing that its business will be taken up by another registered provider, as well as of its name. The notification is published on Evrotrust's website;
- notifies the clients of the conditions of maintenance of the data objects by the taking up Provider;
- changes the status of the operational certificates and hands over duly all the documentation related to its business to the taking up Provider;
- performs all the necessary actions for transferring any obligations regards the information maintenance to the taking up Provider;

The receiving Provider takes up the rights and obligations of Evrotrust with terminated business and continues the qualified preservation service management.

The archive of Evrotrust with terminated status has to be handed over to the Provider having taken up the business.

5.10.2 REVOCATION OF THE QUALIFIED STATUS OF EVROTRUST OR OF THE QUALIFIED STATUS OF THE QUALIFIED PRESERVATION SERVICE

In case of revocation of the qualified status of Evrotrust or of any of the trust services provided by it, it performs the following:

- notifies its users of its changed status or of that of the qualified preservation service;
- changes the status of its certificates;
- terminates the provision of the qualified preservation service but continues preserving and managing the data objects for the document preservation period stipulated by the law;

- make reasonable business efforts for minimizing the violation of the clients' interests.

6 MANAGEMENT OF TECHNICAL SECURITY

6.1 GENERATION AND INSTALLATION OF KEY PAIRS

The procedure for generating and installing the key pairs of the "Evrotrust Services CA" and the signatory of "Evrotrust QERDS SU" follows the procedures described in paragraph 6 of the document "Practice of Qualified Certification Services."

6.2 PROTECTION OF PRIVATE KEYS AND CRYPTOGRAPHIC MODULE

Evrotrust has built security controls for the management of all cryptographic keys and cryptographic devices throughout their life cycle.

Evrotrust, generates a Qualified Electronic Seal Certificate, which uses for its QPSES provision activities. The private key of the electronic seal certificate is stored in a physically isolated premise and only authorized trusted staff has access to the keys. The private key is stored and used within a secure environment for the performance of cryptographic operations. This key is only archived, stored, and restored by employees with trusted roles in a physically secure environment. The number of staff authorized to perform this function is minimized and consistent with the QERDS practice. The private key for stamping by QPSES is stored in a secure environment and may not be taken out of it unprotected. The number of staff authorized to perform this function is kept to a minimum and is in line with QPSES practice.

The management of the keys used to generate and validate the evidence is subject to special requirements. Evrotrust ensures that the time stamps used in the storing process come from the "Evrotrust TSA", which meets the most up-to-date security requirements, and in particular ETSI EN 319 421. Evrotrust only uses time stamping processes, which can be verified using CRL or OCSP responses, and which include "reason code" in the event of suspension / termination of a certificate.

6.2.1 USED ALGORITHMS

All used algorithms are in compliance with the ETSI TS 119 312 technical specification. Evrotrust regularly monitors the security and applicability of the used hash algorithm. All algorithms used are checked once a year or when changes occur. If the algorithm is compromised or becomes inappropriate, proceed to the regeneration of all the keys involved. For each supported storage profile, Evrotrust monitors the strength of each cryptographic algorithm used in connection with this account. In the event that one of the algorithms or parameters used is considered to be less certain or the validity of the corresponding certificate expires, it updates the policy or creates a new preservation profile.

6.3 OTHER ASPECTS OF THE MANAGEMENT OF KEY PAIRS

The procedure for management of key pairs of the Evrotrust Services CA and the signatory of QERDS SU follows the procedures described in paragraph 6.2 of the document "Practice of Qualified Certification Services."

6.4 ACTIVATION DATA

The procedure for activation of key pairs of the Evrotrust Services CA and the signatory of QERDS SU follows the procedures described in paragraph 6.2 of the document "Practice of Qualified Certification Services."

6.5 COMPUTER SECURITY

The security procedure for computer systems is described in paragraph 6.5 of the document "Practice of Qualified Certification Services."

6.6 SECURITY OF THE TECHNOLOGY SYSTEM LIFE CYCLE

The security procedure for computer systems is described in paragraph 6.6 of the document "Practice of Qualified Certification Services."

6.6.1 INFORMATION SYSTEM VULNERABILITY ASSESSMENT

The procedure for assessing the vulnerability of the information system is described in section 6.6.3 of the document "Practice of Qualified Certification Services."

6.7 NETWORK SECURITY

The procedure for network security is described in paragraph 6.7 of the document "Practice of Qualified Certification Services."

Qualified preservation service is integrated into the IT environment so that any change in the contents of the preserved user / client data packet is made only by QPSES.

6.8 TIME STAMP

Description of the process of generating time stamps, managing the process of generating time stamps, participants in the process of issuing and maintaining customized electronic time stamps, their responsibilities, rights and obligations, the applicable range of electronic time stamps are described in the "Policy and Practice of a Qualified Electronic Time Stamps Service " document.

7 VALIDATION DATA OF QUALIFIED CERTIFICATES, CRL AND OF OCSP

7.1 PROFILE OF CERTIFICATION AUTHORITY „EVROTRUST SERVICES CA"

"Evrotrust Services CA" with OID: 1.3.6.1.4.1.47272.2.14 is the qualifying authority of the qualified electronic signature / seal preservation service, which certifies the documents / evidence generated under this policy.

Version	V3	
Serial number	38 00 00 00 07 58 f6 72 2b 87 3d 45 0d 00 00 00 00 00 07	
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	10 July 2019, 12:50:59 UTC	
Validit to	10 July 2029, 13:00:59 UTC	

Subject	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Public Key Type/Length	RSA (4096 Bits)	
Subject Key Identifier	1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
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	
Subject Alternative Name	RFC822 Name=servicesca@evrotrust.com URL=http://www.evrotrust.com	
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	

Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=0

Thumbprint (SHA1): 7448b95dc14ff7127af731c580e0d6ca74f3fe10

Thumbprint (SHA256):

5c7ac0f5ada82e251b4cb8d701a43a4a5baf369289d4f29e27ab2690a88162ec

7.2 PROFILE OF CERTIFICATE STATUS AUTHORITY „EVROTRUST SERVICES VALIDATION“

The qualified certificate for qualified electronic seal of „Evrotrust Services Validation“ is:

Version	V3	
Serial number	6F7071A6CAB1839E4C978A68D7068768F7331E31	
Signature Algorithm	SHA256RSA	
Valid from	Jan 18 07:11:57 2024 GMT	
Validit to	Jan 16 07:11:56 2029 GMT	
Issuer	CN=	Evrotrust Services CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust Services OCSP 2024
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	71D54D65955A8D93762399B91E398B3DABBE8208	
Key Usage (critical)	Digital Signature, Non Repudiation (c0)	
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	
Authority Key Identifier	KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E	
OCSP No Revocation Checking	NULL	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.crl	
Certificate Policies	[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1.47272.2.14.1 [1,1]Policy Qualifier Info:	

<table>
<tr><td></td><td colspan="2">Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>Authority Key Identifier</td><td colspan="2">KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E</td></tr>
<tr><td>CRL Distribution Points</td><td colspan="2">[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://services.evrotrust.com/EvrotrustServicesCA.crl</td></tr>
<tr><td>Authority Information Access</td><td colspan="2">[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</td></tr>
<tr><td>Basic Constraints (critical)</td><td colspan="2">Subject Type=End Entity
Path Length Constraint=None</td></tr>
<tr><td rowspan="5">QCStatements</td><td>id-qcs-pkixQCSyntax-v2[i]
(oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-<b>Legal</b>
(oid=0.4.0.194121.1.2)</td></tr>
<tr><td colspan="2">id-etsi-qcs-<b>QcCompliance</b>
(oid=0.4.0.1862.1.1)</td></tr>
<tr><td colspan="2">id-etsi-qcs-<b>QcSSCD</b>
(oid=0.4.0.1862.1.4)</td></tr>
<tr><td>id-etsi-qcs-<b>QcType</b>
(oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-<b>eseal</b> (oid=0.4.0.1862.1.6.2)</td></tr>
<tr><td>id-etsi-qcs-<b>QcPDS</b>
(oid=0.4.0.1862.1.5)</td><td>PdsLocations

PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
language=en</td></tr>
</table>

Thumbprint SHA1: E1CBEE3169AE35A4E3C842B91A962F1B9DD8BFA3

Thumbprint SHA256:

95D9B9BDDF5CD372E84E02AC52A38592ADE3453DC5CE0904AE75E8CA35227705

7.3 CRL PROFILE OF „EVROTRUST SERVICES CA"

The list of canceled and terminated certificates (CRL) of the certification authority for the qualified electronic registered delivery service "Evrotrust Services CA" has the folowing profile:

Version	V2	
Issuer	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Effective date	[effective UTC date and time of the valid issued CRL]	
Next update	[UTC date and time of planned next update of the CRL]	
Signature Aagorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
CRL Number	[sequential CRL number]	
ExpiredCertsOnCRL	[starting date of revocation status information for expired certificates]	

7.4 PROFILE OF „EVROTRUST QPSES SU"

The qualified certificate for qualified electronic seal of „Evrotrust QPSES SU" is:

Version	V3	
Serial number	2431EA3C6AF78F7FB99638D49804FC63BA1DD5E9	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Valid from	Jan 18 07:19:41 2024 GMT	
Validit to	Jan 16 07:19:40 2029 GMT	
Subject	CN=	Evrotrust QPSES SU 2024
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC

<table>
<tr><td></td><td>C=</td><td>BG</td></tr>
<tr><td>Public Key Type/Length</td><td colspan="2">RSA (2048 Bits)</td></tr>
<tr><td>Authority Key Identifier</td><td colspan="2">KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E</td></tr>
<tr><td>Authority Information Access</td><td colspan="2">[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</td></tr>
<tr><td>Certificate Policies</td><td colspan="2">[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.13
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>QCStatements</td><td colspan="2"><table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-<b>Legal</b> (oid=0.4.0.194121.1.2)</td></tr>
<tr><td colspan="2">id-etsi-qcs-<b>QcCompliance</b> (oid=0.4.0.1862.1.1)</td></tr>
<tr><td colspan="2">id-etsi-qcs-<b>QcSSCD</b> (oid=0.4.0.1862.1.4)</td></tr>
<tr><td>id-etsi-qcs-<b>QcType</b> (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-<b>eseal</b> (oid=0.4.0.1862.1.6.2)</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>id-etsi-qcs-<b>QcPDS</b>
(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>AA329A30B8C7A87B6AED6578BB9E481DEBD1201D</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): 1C4AD99D92746AC6BD1CC8524E2F32ED7749F249

Thumbprint (SHA256):

B2BDCB1180ECE8436A499DB185431A4FECA1F84BA431CA72FBF5B7F1998E6324

8 OTHER BUSINESS AND LEGAL ISSUES

8.1 TARIF

Evrotrust maintains a document entitled "Tariff for trust, information, cryptographic and consulting services" on its website: https://www.evrotrust.com.

8.2 FINANCIAL RESPONSIBILITY

Evrotrust shall be financially liable to QPSES customers who rely on its business. The financial liability shall only be applicable if the damage is due to the fault of Evrotrust or the parties with which it has concluded an agreement. If Evrotrust confirms and accepts that damage has occurred, it undertakes to pay the damages. The maximum payment limit shall not exceed the amount of damage.

The financial liability of each person involved in QPSESS provision and use activities shall be indicated by mutual agreements.

8.3 PERSONAL DATA PRIVACY

Evrotrust is registered as a personal data controller under the terms of the Personal Data Protection Act.

As a personal data controller, Evrotrust strictly respects the requirements for the confidentiality and non-disclosure of personal data of natural and legal persons that have come to its knowledge in the performance of its activities as a qualified trust service provider.

1) The company uses in its activities:

➢ only such information about the activities and the business of its customers and partners that is required to provide QPSES;

➢ confidential information such as commercial, financial and technical documents (software, analyzes, tables, data, surveys, prices, contracts and other documents).

2) Evrotrust informs its employees:

➢ with the obligation that the company's interest shall be a priority over personal interests and that employees shall do their best to avoid causing damage;

➢ of the provisions of the Personal Data Protection Act and the European legislation on personal data protection, as well as the measures and procedures for the protection of personal data in the company;

➢ that all data and information defined as constituting trade secret shall be carefully stored to prevent disclosure without the express permission of the provider;

➢ that they are obliged to collect personal data regardless of the ethnicity of the person to whom they relate and regardless of their form and location. They are obliged to protect the data from deliberate or accidental destruction, deletion, transmission to third parties or other type of processing of such data;

➢ that processing of personal data (collection, storage, modification, transmission, deletion and any type of processing related thereto) is only permitted in cases where there is legal grounds for such processing in accordance with national legislation governing the protection of personal data and that any other type of processing is illegal;

- that unauthorized disclosure of confidential information lies at the root of the cessation of cooperation;
- that the issuance and unwarranted acquisition of professional secrecy constitutes a crime;
- that misuse of personal data constitutes a crime.

8.4 INTELLECTUAL PROPERTY RIGHTS

There are various data integrated in the QERDS operated by Evrotrust, which are subject to intellectual property rights and other proprietary or non-proprietary rights.

8.5 OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES

8.5.1 OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES OF EVROTRUST

Evrotrust warrants that it performs its activities by:

- complying with the terms and conditions of this document, the requirements of Regulation (EU) No. 910/2014 and the national legislation;
- its provided QPSES service not infringing the copyrights and licensed rights of any third party;
- using technical equipment and technologies that ensure system reliability and technical and cryptographic security in the performance of the processes, including a secure and protected mechanism/device for generating keys in its infrastructure;
- providing QPSES after verifying the information provided by means permitted by law;
- securely storing and maintaining information related to the QPSES provided and the systems operational performance;
- complying with the established operational procedures and the technical and physical control regulations, in accordance with the terms and conditions of this Policy and Practice;
- providing conditions for the accurate determination of the time of sending and receiving data;
- performing procedures of identification and authentication of natural and legal persons or of authorized representatives of legal persons;

- taking immediate measures in the event of technical security issues;
- informing customers about their obligations and due care in the use of the QPSES certification service provided by Evrotrust;
- using and storing the collected personal and other information only for the purposes of its activities in accordance with the national legislation;
- concluding an insurance for the period of its activities;
- maintaining trusted staff having the necessary expertise, experience and qualifications to perform the activities;
- performing periodic internal audits of the activities of the Certification Authority and the Registration Authority;
- performing external audits by independent auditors and publishing the audit results on its website;
- using in its activities certified software and hardware as well as secure and reliable technology systems;
- providing maximum access to its services (365/24/7), except for the following cases:
  - scheduled and pre-announced technical repairs to the infrastructure;
  - unscheduled technical repairs to the infrastructure as a result of unforeseen failures;
  - maintenance due to infrastructure failures beyond the provider's jurisdiction;
  - inaccessibility of the service as a result of force majeure or extraordinary events.
- declaring the maintenance or upgrading of its infrastructure at least three (3) days prior to the commencement of the repair.

Evrotrust is liable to its customers for any damages caused by gross negligence or intent:

- resulting from failure to comply with the requirements of Regulation (EU) No. 910/2014 in the performance of its QPSES provision activities;
- resulting from failure to comply with its obligations to provide QPSES.

8.5.2 OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES OF THE REGISTRATION AUTHORITY

Evrotrust warrants that the Registration Authority performs its functions and obligations in full compliance with the terms and conditions of this document, with the requirements and procedures in the Policy and the internal operational instructions issued.

Evrotrust shall be responsible for the activities of the Registration Authority in its infrastructure.

Evrotrust warrants that the Registration Authority:

- ➢ performs its activities using reliable and secure devices and software;
- ➢ provides services that are in compliance with the national legislation and do not infringe any customer's copyright and licensed rights;
- ➢ makes the necessary efforts to perform correct identification of customers, where necessary.

8.5.3 OBLIGATIONS OF CLIENTS (SUBSCRIBER)

The natural and legal persons (clients) have the following obligations:

- ➢ To get acquainted with and comply with the conditions of the Agreement, General conditions, Policies and Practice Statements while using QPSES, as well as the requirements in the rest of the documents published of Evrotrust's website;
- ➢ To use the qualified preservation service for lawful purposes only and in compliance with the Policy and Practice Statement appointed for it;
- ➢ To approve the conditions set out in the Agreement between them and Evrotrust. The Agreement specifies who is entitled to access to the preserved objects, including submitted data objects and evidence. It specifies who is entitled to monitor the actions related to the preserved objects.

8.6 RELEASE FROM LIABILITY

Evrotrust IS NOT liable for damages arising from:

- ➢ the use of QPSES beyond the limits of its listed intended uses and restrictions of its operation;

- illegal actions by customers;
- accidental events having the nature of force majeure, including malicious actions of third parties (hacker attacks, depriving of the device for the use of the electronic registered delivery, of the identification method, etc.);
- the use of electronic registered delivery in non-compliance with the requirements and procedures of the Evrotrust Practice and Policy;
- incorrect and inadequate password protection;
- the disclosure of confidential data and irresponsible behaviour by customers;
- damage to the infrastructure beyond Evrotrust's area of management;
- inadequate customer behaviour when using the QERDS service.

8.7 LIMITATION OF LIABILITY

For the qualified service of electronic registered delivery, Evrotrust sets a liability limit of EUR 5,000.

8.8 INSURANCE

Evrotrust concludes a compulsory insurance for its activities as a qualified trust service provider.

8.9 TIME AND TERMINATION OF POLICY AND PRACTICE

This document becomes effective as soon as it is approved by the Board of Directors of Evrotrust and published of the Evrotrust website. Appendices to this Policy and Practice take effect after their publication.

The provisions in this document are valid until the next version of "Policy and Practice of Qualified Long Term Preservation Service" is published on the Evrotrust website.

Upon termination of the operation of Evrotrust, the topicality of the Policy and Practice, as well as the provisions contained in this document, are terminated.

The Provider keeps all previous versions / editions of this document duly and securely.

8.10 INDIVIDUAL MESSAGES AND MESSAGES WITH PARTICIPANTS

Persons referred to in this Policy and Practice can make statements and exchange information using ordinary post, e-mail, fax, telephone and network protocols (such as TCP / IP, HTTP) and through the Evrotrust mobile application.

The choice of funds can be chosen depending on the type of information and the way the service is used.

8.11 POLICY AND PRACTICE AMENDMENTS

Changes in this document may result from observed errors, updates and suggestions from affected parties. In the event of an invalid Policy and Practice clause, the validity of the entire document is retained and the contract with the customer is not violated. The invalid clause is replaced by a legal norm.

Evrotrust may make editorial changes to this document that do not affect the content of the rights and obligations contained therein. In the event of changes to Policy and Practice, the Object Identifier of the document (OID) is retained and does not change. Changes that lead to a new version of the document are published on the Evrotrust website.

8.12 DISPUTE SETTLEMENT

Any disputes or complaints concerning the use of QERDS provided by Evrotrust shall be settled through mediation on the basis of written information. Complaints shall be dealt with by the legal adviser of Evrotrust. Any complainant will receive a reply within 2 (two) business days after the submission thereof. In the event that no resolution is found for a dispute within 30 (thirty) days of the commencement of the settlement procedure, the parties may refer the dispute to the Bulgarian court.

8.13 APPLICABLE LAW

For all matters not covered by this document the provisions of the Bulgarian legislation shall apply.

8.14 COMPLIANCE WITH APPLICABLE LAW

Where possible, the qualified preservation service for qualified electronic signatures/seals is accessible to disabled people.

Evrotrust guarantees that the service operates in a lawful and reliable manner. It is offered in compliance with applicable legal requirements. The provisions of the Bulgarian legislation apply to all matters unsettled herein. Should the national legislation change, the legal rules will be effective until this policy is harmonized. Evrotrust's business complies with the applicable ETSI EN 301 549 standard: Requirements for accessibility suitable for public tenders of information and communication technology products and services in Europe.

Evrotrust guarantees that personal data is processed in compliance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL 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/GDPR). Evrotrust has undertaken appropriate technical and organizational measures against unauthorized or unlawful personal data processing, as well as against accidental personal data loss, destruction or damage. In that respect the online authentication service refers only to the processing of identification data, which is adequate, reasonable and minimum necessary for providing access to the service.

8.15 GENERAL PROVISIONS

The obligations and responsibilities of consumers and Evrotrust are governed by contractual agreements. Relationships with trustworthy parties are governed by general law. Contracts for the provision of qualified electronic registered delivery services should be concluded in written or electronic form, subject to the provisions of Regulation (EU) No 910/2014, REGULATION (EC) 2016/679 and the applicable legislation in the Republic of Bulgaria.

8.16 OTHER PROVISIONS

The practice does not specify any other provisions.

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.