CERTIFICATION PRACTICE STATEMENT

FOR QUALIFIED TRUST SERVICES

CONTENTS

1. INTRODUCTION

"Evrotrust Technologies" AD (Evrotrust) is a legal entity, registered in the Commercial Register to the Registry Agency with UIC 203397356, with seat and management address: Sofia city, region Izgrev, r.d. Iztok, 2 Nikolay Haytov Str, entr. D, fl.2. Contact telephone + 359 2 448 58 58. Internet address: http://www.evrotrust.com.

The company conducts public functions under the meaning of the Law on Electronic Document and Electronic Trust Services (LEDETS).

Evrotrust is a supplier of qualified certification services. It provides to clients qualified certification services and products with high degree of security against remuneration. The supplier provides its services both on the territory of the Republic of Bulgaria and in all member-states of the European Union and other countries worldwide.

Innovative in its business, Evrotrust provides users with the opportunity to generate remote electronic signatures/seals. In this cost-effective working method the electronic signature/seal generation medium is managed by the provider on behalf of the Owner/Creator of the electronic signature/seal. Evrotrust guarantees the application of standard security and management procedures and uses reliable systems and products, including secure electronic communication channels in order to guarantee the reliability of the medium where electronic signatures/seals are generated, and to guarantee that the medium is used solely under the supervision of the Owner/Creator of the electronic signature/seal.

1.1 REVIEW

Certification Practice Statement" (Certification Practice Statement/CPS) of Evrotrust Technologies AD is a public document. It can be changed at any time by Evrotrust and every new edit is communicated to the third parties by an updated document published on the website of Evrotrust.

The Certification Practice Statement of Evrotrust describes the general requirements for provision of qualified certification services. The document contains rules and procedures which should be complied with when issuing and managing (stopping, termination and renewal) the effect of qualified certificates for electronic signatures and seals, as well as qualified electronic time-stamps and qualified certificates for websites. During the management process the necessary documents are collected upon admission and inspection of the application for issuing qualified certificates for electronic signatures and stamps, electronic time-stamps, as well as those stored by the supplied, depending on the requested service.

The Certification Practice Statement describes realization of the security measures during provision of the qualified certification services provided by Evrotrust.

This document specifies the rights and obligations of both the participants in the Public Key Infrastructure (PKI) of the supplier, and of all external persons (if any), participating in the activities for provision of qualified certification services. The responsibilities, rights and obligations of the signatory are also described, as well as those of the developer of the qualified electronic signature and stamp when using the certification services provided by Evrotrust.

This document contains description of the following provided by Evrotrust services:

- Issuing and management of qualified certificates for elaborated and qualified electronic signatures/seals;
- Issuance and management of qualified certificates for website;
- Issuance and management of a qualified electronic time stamp;

Evrotrust can provide cryptographic, informational and consulting services related to the applicability of the certification services, in compliance with the generally accepted recommendations, specifications and standards. Evrotrust can publish separate General Conditions for these services.

The Certification Practice Statement is related to all participants in the Public Key Infrastructure of Evrotrust all over the world, including certification authorities, registration authorities, trade agents, users, end users and all relying parties.

Certification services are provided in accordance with the Integrated Management System implemented by Evrotrust, which includes the requirements of ISO 9001[1], ISO 27001[2], ISO

[1] *ISO 9001 Quality Management Systems;*

[2] *ISO 27001 Information Technologies. Security Methods. Information Security Management Systems;*

22301[3], ISO 20000-1[4], EU Regulation № 910/2014[5], EU Regulation № 2016/679[6] (GDPR), EU Directive 2015/2366[7] (PSD2), and the applicable legislation of the Republic of Bulgaria.

This document is structured in compliance with the framework defined in recommendation IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

Evrotrust supports a number of documents associated with the implementation of the Practice. Some of them are not publicly accessible because they are part of the security of Evrotrust information management system.

1.2 PRACTICE REQUIREMENTS

Evrotrust applies the following general requirements:

a) Evrotrust applies a set of policies and practices appropriate to the remote electronic signature/seal service. The applicable policies and practices are listed, together with their object identifiers, in the issued certificates when using the service. For each certification service provided and each certificate issued, Evrotrust has published on its website a policy and practice with included object identifiers;

b) The management of Evrotrust approves the set of policies and practices and they are thereafter published and communicated to the employees and relying parties, where appropriate;

c) This document describes the practices and procedures used to address all requirements of the applicable trust service policy as identified by the Evrotrust;

d) This document, in item 1.5.5 thereof, refers to the possibility of involving external organizations supporting the services of Evrotrust. In the case of external organizations, their

[3] *ISO 22301 Security of Society. Business Continuity Management Systems;*

[4] *ISO 20000-1 IT Service Quality Management System;*

[5] *European Parliament and Council Regulation № 910/2014 dated 23rd of July, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;*

[6] *European Parliament and Council Regulation № 2016/679 dated 27th of 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);*

[7] *European Parliament and Council Directive 2015/2366 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and EU Regulation No 1093/2010, and repealing Directive 2007/64/EC;*

obligations and applicable policies and practices shall be described in contractual agreements;

e) Evrotrust shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to demonstrate conformance to the trust service policy;

f) When Evrotrust intends to make changes in its Practice that could affect the acceptance of the service by the subject, subscriber or relying parties, Evrotrust shall duly subscribers or relying parties of the changes by publishing the updated Practice;

g) Evrotrust has a management body that finally approves this document;

h) The management of Evrotrust manages the implementation of the applicable policies and practices;

i) Evrotrust defines the practices review process which takes place at least once a year, and defines the responsibilities for their maintenance which it assigns to authorized personnel;

j) Evrotrust promptly updates the practices and policies, with each new version of the documents being approved by the management and published on the company's website;

k) Evrotrust publishes each new edition of its applicable practices and policies without delay;

l) Termination of the service may occur upon termination or expiration of the trust services agreement entered into between a user and Evrotrust. An agreement may be terminated upon closing a user profile. Item 5.9 of this document stipulates the provisions for termination of an agreement upon termination of the business of Evrotrust.

1.3 REGULATORY REFERENCES

The contents and structure of this document are in compliance with the following standards and standardization documents:

- RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile;
- RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;

- RFC 3161 Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP);
- RFC 5816 ESSCertIDv2 Update for RFC 3161;
- RFC 3279 Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile;
- RFC 4055 Additional Algorithms and Identifiers for RSA Cryptography for use in the ` X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;
- ITU-T X.509 | ISO/IEC 9594-8: The Directory: Authentication framework; Public-key and attribute certificate frameworks
- ETSI EN 319 401 „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates General requirements;
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates Requirements for trust service providers issuing EU qualified certificates;
- EN 319 421 v1.1.1 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 412-1 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;“;
- ETSI EN 319 412-2 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons;“;
- ETSI EN 319 412-3 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles;Part 3: Certificate profile for certificates issued to legal persons;“;
- ETSI EN 319 412-4 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations;“;
- ETSI EN 319 412-5 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements;“;
- EN 319 422 Time-stamping protocol and electronic time-stamp profiles;
- TS 119 312 Cryptographic Suites;
- EN 319 521 Policy and Security Requirements for Electronic Registered Delivery Service Providers;
- EN 319 522 Electronic Registered Delivery Services;
- EN 319 531 Policy and Security Requirements for Electronic Registered Electronic Mail

Service Providers;

- EN 319 532 Registered Electronic Mail (REM) Services;
- ETSI TS 119 495: „Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366".

1.4 NAME AND DOCUMENT IDENTIFICATION

The full name of this document is "Qualified Certification Practice Statement" by "Evrotrust Technologies" AD and is publicly accessible in electronic version on the website of EVROTRUST: https://www.evrotrust.com/landing/bg/a/tsp-documents or is provided after preliminary request sent to e-mail: office@Evrotrust.com.

The Practice has assigned unique object identifier (OID – Object Identifier) 1.3.6.1.4.1.47272.3.1.1.

The Practice is related to the policies for provision of qualified certifications for electronic signatures and stamps and qualified certification services.

Policies includes:

- description of the conditions which Evrotrust complies with and observes when issuing qualified certificates, as well as applicability of these certificates considering the security level and limitations during their use.
- a set of specific procedures which are complied with during the process of issuing and maintaining qualified certificates, requirements during identification, conditions and necessary levels of security during creation of the electronic signature/stamp and storage of the private key.
- specifies the applicability and degree of trust in the applied information in the qualification certificates.

The Practice executes the general requirements for certification policies described in ETSI EN 319 411-1: NCP; NCP+; NCP; NCP+, DVCP and OVCP.

The practice meets the general requirements for certification policies set out in ETSI EN 319 411-1:

1. **NCP** - Normalized authentication policy, which corresponds to the generally recognized best practices of certification-service providers used to support all types of transactions.

2. **NCP +** - Extended normalized authentication policy, which offers the quality of NCP, but

also includes the requirements for a secure cryptographic device.

3. **LCP** - A policy for lightweight certificates that offers quality of service with fewer requirements for use by NCPs, such as no physical presence required. Applies to certificates used to support any type of transaction (such as digital signatures, web authentication).

4. **EVCP** - Extended policy for validation of TLS / SSL certificates, offering the level of security required by the CAB Forum. The requirements are based on the requirements of NCP certificates, but supplemented by the requirements of EVCG.

5. **DVCP** - Domain Authentication Policy (DVCP) for TLS / SSL certificates, offering the level of security required by the CAB Forum. The policy requirements are based on the requirements of the LCP, but supplemented by the requirements of the BRG.

6. **OVCP** - TLS / SSL Certification Policy for Organizations, offering the level of security required by the CAB Forum. The policy requirements are based on the LCP but supplemented by the requirements of the BRG.

7. **IVCP** - Individual Certificate Validation Policy (IVCP) for TLS / SSL certificates, offering the level of security required by the CAB Forum. The policy requirements are based on the LCP requirements, supplemented by the BRG requirements.

Evrotrust certification policies comply with the rules set out in ETSI EN 319 411-1 and the identifiers for each policy. Evrotrust issues certificates applying the following policies:

a) normalized certification policy (**NCP**).

b) improved normalized certification policy (**NCP +**) and

c) extended certificate validation policy (**EVCP**).

In its certification activity, Evrotrust applies the following EU qualified certification policies:

1. Policy for certificates issued **to natural persons** (**QCP-n**) complying with EU requirements (policy for NCP, NCP + and additional requirements for qualified certificates, as set out in Regulation (EU) № 910/2014). Certificates issued in accordance with these requirements shall support advanced electronic signatures based on a qualified certificate as defined in Articles 26 and 27 of Regulation (EU) № 910/2014;

2. Policy for certificates issued **to legal entities (QCP-l)** complying with EU requirements (NCP policy, NCP + and additional requirements for qualified certificates as set out in Regulation (EU) № 910/2014). Certificates issued in accordance with these requirements shall support advanced electronic signatures based on a qualified certificate as defined in Articles 26 and 27 of

Regulation (EU) № 910/2014;

3. Policy for Qualified Certificates (**QCP-n-qscd**) issued to individuals using a signature creation device (QSCD) (includes QCP-n, NCP + policy and additional requirements as set out in Regulation (EU) № 910/2014). Such a policy requires the private key to be located in a QSCD that meets the requirements of Regulation (EU) № 910/2014. Such a policy requires the private key to be located in a QSCD that meets the requirements of Regulation (EU) № 910/2014. Certificates issued in accordance with these requirements shall support qualified electronic signatures as defined in Article 3 (12) of Regulation (EU) № 910/2014;

4. Policy for Qualified Certificates (**QCP-l-qscd**) issued to legal entities using a signature creation device (QSCD) (includes QCP-n, NCP + policy and additional requirements as specified in the Regulation (EU) № 910/2014). Such a policy requires that the private key associated with the certified public key be located in the QSCD. Certificates issued in accordance with these requirements shall support qualified electronic seals as defined in Article 3 (27) of Regulation (EU) № 910/2014;

5. Qualified Certificates Policy for Websites (**QCP-w**) meeting the requirements of Regulation (EU) № 910/2014 (requiring or not using a secure cryptographic device):

(a) Where the certificate is issued to a legal person, the requirements for QCP-w shall include all EVCP requirements and additional requirements as set out in Regulation (EU) (910/2014.

(b) When the certificate is issued to a natural person, the requirements for QCP-w include all NCP requirements and additional requirements as specified in Regulation (EU) № 910/2014).

The Practice executes the general requirements for certification policies described in ETSI EN 319 411-2: QCP-l ; QCP-l-qscd; QCP-n; QCP-n-qscd and QCP-w.

Qualification certificates issued by Evrotrust contain policy identifiers: Certificate Policy extension.

Each of the policies with which the qualification certificates from Evrotrust are issued acquire Object Identifier (OID – Object Identifier) and Evrotrust specifies in its policies the identifiers according EN 319 411-1/ EN 319 411-2. The values of the Evrotrust identifiers are:

Qualified body/service	**Object Identifier (OID), Policy identifier**
Evrotrust RSA Root CA	1.3.6.1.4.1.47272.1
Evrotrust RSA Validation (OCSP service)	1.3.6.1.4.1.47272.1.1
Evrotrust TSA	1.3.6.1.4.1.47272.1.2
Evrotrust TST	1.3.6.1.4.1.47272.1.2.1
Evrotrust RSA Operational CA	1.3.6.1.4.1.47272.2
Evrotrust RSA QS Validation (OCSP service)	1.3.6.1.4.1.47272.2.1
Evrotrust Qualified Natural Person Certificate for QES	1.3.6.1.4.1.47272.2.2
Evrotrust Qualified Natural Person Attribute Certificate for QES	1.3.6.1.4.1.47272.2.2.1
Evrotrust Qualified Legal Person Certificate for QESeal	1.3.6.1.4.1.47272.2.3
Evrotrust SSL Domain Validated Certificate	1.3.6.1.4.1.47272.2.4.1
Evrotrust SSL Organization Validated Certificate	1.3.6.1.4.1.47272.2.4.2
Evrotrust SSL EV Certificate	1.3.6.1.4.1.47272.2.5
Evrotrust SSL PSD2 Certificate	1.3.6.1.4.1.47272.2.5.1
Evrotrust Qualified Natural Person Certificate for AES	1.3.6.1.4.1.47272.2.7
Evrotrust Qualified Legal Person Certificate for AESeal	1.3.6.1.4.1.47272.2.8
Evrotrust Qualified PSD2 Legal Person Certificate for AESeal	1.3.6.1.4.1.47272.2.8.1
Evrotrust Services CA	1.3.6.1.4.1.47272.2.14
Evrotrust Services Validation (OCSP service)	1.3.6.1.4.1.47272.2.14.1

Evrotrust reserves its right to broaden the maintained Policies of issued certificates through the operational Certification Bodies.

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.

1.5 PARTICIPANTS IN THE INFRASTRUCTURE OF EVROTRUST

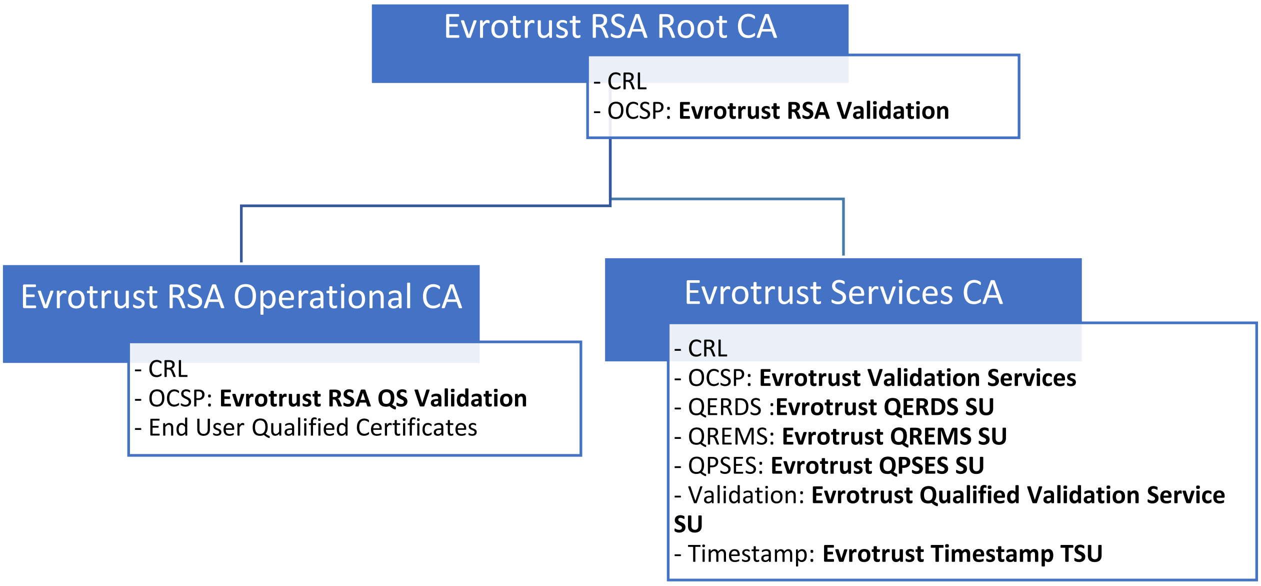
The Practice regulates the most important relations between the participating parties in the structure of Evrotrust, its consultants and auditing teams, as well as he relations between the supplier, the users of qualified certification services and the relying parties. The requirements and rules described in the Practice are applied for:

- Certification authorities;
- Registration authorities;
- Users (Clients/Subscribers / Signatories / Creators, etc.);
- Relying parties;
- Other participants.

Evrotrust provides qualified certification services to all natural and legal persons who agree with the rules of this document. The aim of the Practice is that the clients are assured in the security of the provided qualified certification services.

1.5.1 CERTIFICATION AUTHORITIES

1.5.1.1 HIERARCHY OF THE AUTHORIZING AUTHORITY


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**

1.5.1.2 ROOT CERTIFICATION AUTHORITY („EVROTRUST RSA ROOT CA“)

„Evrotrust RSA Root CA“ issues qualified electronic certificates which are hierarchically dependent in infrastructural relation in the domain of Evrotrust. The root certificate of Evrotrust is issued and signed automatically with the root private key of Evrotrust. The supplier signs certificates for public keys of its operational Certification authorities with the root private key.

1.5.1.3 OPERATIONAL CERTIFICATION AUTHORITY („EVROTRUST RSA OPERATIONAL CA“)

„Evrotrust RSA Operational CA“ issues user qualified certificates in accordance with the Practice and Policy for provision of qualified certification services.

The user qualified certificates issued by „Evrotrust RSA Operational CA“ in the infrastructure of Evrotrust are:

- **Evrotrust Qualified Natural Person Certificate for QES/AES (E-Sign)** - issued to a natural person (Signatory). It has the nature of a qualified certificate for qualified electronic signature/advanced electronic signature QES/AES. It can be used for identification and establishing identity when accessing internet applications, secured communications and electronic signing of any type of documents. The certificate can also include data of a legal entity, associated with natural person, on behalf of which the Signatory will sign.
- **Evrotrust Qualified Legal Person Certificate for QESeal/AESeal (E-Seal)** - issued to a legal entity (Creator). It has the nature of a qualified certificate for qualified electronic stamp/advanced electronic stamp (QEStamp/AEStamp). It can be used to guarantee the origin and integrity of outgoing data by the legal entity, for example: electronic documents, pictures, architectural projects, software, etc.
- **Evrotrust Qualified PSD2 Legal Person Certificate for AESeal (E-Seal)** – issued to payment service providers (PSP) under PSD2. It constitutes a qualified certificate for AEStamp. It is used to meet the requirements of PSD2.
- **Evrotrust SSL Domain Validated/Organization Validated/EV Certificate (Website authentication)** – issued for the purpose of authentication of websites related to a given natural or legal person. It constitutes a qualified website authentication certificate within the meaning of Regulation (EU) No 910/2014 and is used to assure website visitors that there is a genuine and legitimate entity standing behind the website. The technology secures reliable connectivity through a secure information exchange protocol.
- **Evrotrust SSL PSD2 Certificate (Website authentication)** – issued for the purpose of authentication of websites related to payment service providers (PSP) under PSD2. It is used to meet the requirements of PSD2. It constitutes a qualified website authentication certificate within the meaning of Regulation (EU) No 910/2014 and is used to assure website visitors that there is a genuine and legitimate entity standing behind the website. The technology secures reliable connectivity through a secure information exchange protocol.

- **Evrotrust Qualified Natural Person Attribute Certificate for QES** - issued in order to identify a natural person (Signatory) with attributes, which are specific and are described in the certificate. It has the nature of a qualified certificate for QES. All the procedures and rules that are followed during its issuance and maintenance is the same as for the „Evrotrust Qualified Natural Person Certificate for QES/AES (E-Sign)". The difference between them is in the validity period, the scope and the type of the certified data.

The qualified operational certification authority of Evrotrust executes the following specific obligations included in the Policy and Practice of Evrotrust:

- ➢ Approval of electronic request for qualified certificates or qualified certification services;
- ➢ Issuing qualified certificate and qualified certification service based on the requirements after identification of the users;
- ➢ Publishing and maintaining issued qualified certificates in compliance with the procedures described in the Policy and Practice of Evrotrust;
- ➢ Approval and execution of request for revocation of qualified certification service in compliance with the procedures described in the Policy and Practice of Evrotrust;
- ➢ Issuing a Certificate Revocation List (CRL);
- ➢ Publishing the issued Certificate Revocation List (CRL);
- ➢ Stores the records (logs) on the process for issuing qualified certification services, which are subject to audit;
- ➢ Other activities and services related to the activity of Evrotrust.

Evrotrust reserves the right to broaden or change its infrastructure with another hierarchy or to extend of the current one.

1.5.1.4 OPERATIONAL CERTIFICATION AUTHORITY (EVROTRUST SERVICES CA)

Evrotrust Services CA issues user qualified certificates in accordance with the Practice and Policy for provision of qualified certification services.

The specialized qualified certificates issued by „ Evrotrust Services CA" in the infrastructure of Evrotrust are:

- **„Evrotrust Timestamp TSU 2024"** - issued to the timestamping signing unit (Timestamp Signing Unit/TSU) of the qualified time stamp authority "Evrotrust TSA" and is intended to proof the exact date and time of an electronic signature or other event. The full description of the service and the profile of the issued certificate can be found in the document "Policy and practice for qualified electronic time stamp provisioning service";

- **"Evrotrust QERDS SU 2024"** – issued to the signing unit (Signing Unit/SU) of the qualified electronic registered delivery service (QERDS) is intended to proof all the issued by the service assertions/evidences. The full description of the service and the profile of the issued certificate can be found in the document "Qualified electronic registered delivery service policy and practice";
- **"Evrotrust QREMS SU 2024"** – issued to the signing unit (Signing Unit/SU) of the qualified electronic registered mail service (QREMS) is intended to proof all the issued by the service assertions/evidences. The full description of the service and the profile of the issued certificate can be found in the document "Qualified electronic registered mail service policy and practice";
- **"Evrotrust QPSES SU 2024"** – issued to the signing unit (Signing Unit/SU) of the Qualified preservation service for qualified electronic signatures / seals (QPSES) is intended to proof all the issued by the service assertions/evidences. The full description of the service and the profile of the issued certificate can be found in the document "Qualified preservation service for qualified electronic signatures / seals policy and practice";
- **„Evrotrust Qualified Validation Service SU 2024"** – issued to the signing unit (Signing Unit/SU) of the Qualified validation service of qualified electronic signatures/seals (QSVSP) is intended to proof all the issued by the service assertions/evidences. The full description of the service and the profile of the issued certificate can be found in the document "Policy and practice for qualified validation service of qualified electronic signatures/seals".

The qualified operational certification authority of Evrotrust "Evrotrust Services CA" executes the following specific obligations included in the Policy and Practice of Evrotrust:

- ➢ Approval of electronic request for qualified certificate for a provided trust service;
- ➢ Issuing a qualified certificate for a provided trust service;
- ➢ Publishing and maintaining issued qualified certificates in compliance with the procedures described in the Policy and Practice of Evrotrust;
- ➢ Approval and execution of request for revocation of a qualified certificate in compliance with the procedures described in the Policy and Practice of Evrotrust;
- ➢ Issuing a Certificate Revocation List (CRL);

- ➢ Publishing the issued Certificate Revocation List (CRL);
- ➢ Stores the records (logs) on the process for issuing qualified certification services, which are subject to audit;
- ➢ Other activities and services related to the activity of Evrotrust.

Evrotrust reserves the right to broaden or change its infrastructure with another hierarchy or to extend of the current one.

1.5.1.5 AUTHORITY FOR INSPECTION OF CERTIFICATE STATUS (OCSP SERVICE)

Within the infrastructure of Evrotrust, the qualified certificates used for the signing of the validation request are as follows:

- Evrotrust RSA Validation – Used for validation of the root signature and is issued directly by the Root Certification Authority "Evrotrust RSA Root CA";
- Evrotrust RSA QS Validation – Used for validation of qualified certificates and is issued by the Operational Certification Authority "Evrotrust RSA Operational CA";
- Evrotrust Services Validation – Used for validation of qualified certificates and is issued by the Operational Certification Authority "Evrotrust Services CA".

In the process of validating a qualified electronic signature/seal, the Evrotrust Validation Authority shall confirm the validity of the qualified electronic signature/seal if:

- ➢ the certificate attached to the signature/seal by the time of signing/sealing was a qualified certificate of electronic signature/seal meeting the requirements of EU Regulation № 910/2014;
- ➢ the qualified certificate issued by Evrotrust was valid by the time of signing;
- ➢ the signature/seal validation data corresponds to the data provided by the relying party;
- ➢ the unique set of data presenting the Signatory/Creator of the electronic signature/seal in the certificate has been duly submitted to the relying party;
- ➢ the relying party has clearly indicated that an alias had been used by the time of signing;
- ➢ the electronic signature/seal has been generated by a device for the creation of an electronic signature/seal;
- ➢ the integrity of the signed data is not jeopardized;

- the requirements of this document have been met by the time of signing;

The system used by Evrotrust for the validation of qualified electronic signature/seal provides the relying party with the correct result of the validation process and enables it to detect potential security related issues.

When accepting a qualified certificate, each relying party may request a real time verification of the certificates' status through an OCSP server (On-line Certificate Status Protocol/Protocol for certificate's status online verification).

The real time verification of a certificate is not a mandatory function for the relying parties, but the use of this service is recommended by Evrotrust. In order to achieve a higher level of security in the use of electronic signatures/seals, it is advisable to have the service integrated in the process of creating or accepting documents that are electronically signed.

1.5.2 REGISTRATION AUTHORITY

The functions of the Registration Authority are executed by a separate structure of Evrotrust or by external persons, to which Evrotrust assigns their realization, within the scope permitted by the law. These functions are:

- Approves request for qualified certification service;
- Evrotrust shall collect and validate either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation;
- Verification of the subject's identity shall be at time of registration by appropriate means. The collection of evidence may include the copy of personal data, such as ID or passport;
- Identifies the person who submitted a request in accordance with the rules and procedures established by Evrotrust;
- Certifies the veracity and admissibility of a submitted electronic request for qualified certificate;
- Notifies the users for issued qualification certificate;
- Provides reliable environment for receiving the issued qualification certificate or for using qualification certified service;
- Initiates and submits to the certification authorities the requests (these might be in paper or electronic form) for management requests (suspension, renewal or revocation) of issued

certificates;

- Performs approval of requests for continuing the effect of a qualified certificate on behalf of Evrotrust;
- signs contracts for provision of certified and other cryptography, informational and consulting services with the users, on behalf of Evrotrust;
- Other functions guaranteeing the functioning of a qualified certification service of Evrotrust.

The Registration Authority can be a separate unit within a legal entity, different from Evrotrust, to which rights to conduct these activities or part of them on behalf of Evrotrust were delegated. The relations between Evrotrust and Registration Authority are settled by a contract.

1.5.3 USERS

Every natural person, legal entity or other who signed a contract with Evrotrust for qualified certification service is a user of this service, provided by Evrotrust.

When this could be practically conducted, the provided certification services and the products used during provision of the services are also accessible to people with disabilities.

1.5.3.1 SIGNATORY

The signatory is a natural person who creates an electronic signature.

The signatory conducts on their behalf or on behalf of another person they represent, electronic statements, who they sign electronically in compliance with the representative rights granted to them. The person who is represented by the Signatory can be stated in the qualified certificate.

The signatory of the electronic signature can assign the servicing of the tokens for creating qualified electronic signatures to a third party, under the condition that appropriate mechanisms and procedures were implemented, which guarantee that the signatory has sole control on using the data, related to creation of their electronic signature, and that when using the token the conditions regarding the qualified electronic signature were executed.

Only the signatory of the qualified certificate has the right to access the private key for signing electronic statements, through which they create an elaborate or qualified electronic signature.

1.5.3.2 CREATOR OF A SEAL

The creator of a seal is a legal entity, which creates an electronic signature.

The creator can seal electronic objects, regardless of their nature (software, pictures, music, movies, books, architectural projects, data base, design, etc.), with which they manifest that they are the legitimate source of this electronic object and that the object is with intact integrity). The electronic seal does not guarantee rights on the electronic object (copyright or other).

The legal entity is stipulated in the issued qualified certificate for electronic seal as Creator.

Only the Creator in their capacity as User of the qualified certificate, is entitled to access to the private key for stamping electronic statements, through which they create an elaborate or qualified electronic stamp.

1.5.3.3 SUBSCRIBER

A subscriber (client) is the person that uses the qualified trust service. A subscriber may be a legal or a natural person or another entity and may be the same as the Owner/Creator.

A subscriber may act on behalf of one or a few different Owners/Creators with which it has a connection. For example, the subscriber may be a company which requires certificates for its employees in order to enable their participation in electronic business processes on behalf of the company and may not appear in the data shown in the issued certificate. A subscriber may also be a person wishing to use a trust service of Evrotrust to certify time.

1.5.4 RELYING PARTIES

Relying party means a natural person or legal entity who relies on the certification service.

The relying parties should have knowledge and skills regarding the use of the qualified certificate and to trust the certified circumstances in them, considering only the applicable Policy, especially regarding the security level during inspection of the identity of the Signatories and the identity of the Creators of these qualified certificates, as well as regarding the use limitations included in the certificate.

The relying parties have permanent access to the registers of Evrotrust, for inspection of the validity of the qualified certificates, for establishing the electronic identity of the Signatories/Creators, or of other circumstances and data, included in the certificates or these registers.

The relying parties established outside the territory of the Republic of Bulgaria can rely on reliable, secure, easy and comfortable qualified validation of the qualified electronic signatures and electronic stamps in an automated manner, the certificates for which were issued by Evrotrust.

1.5.5 OTHER PARTICIPANTS

For certain activities, pursuant to Regulation (EU) No. 910/2014, Evrotrust may involve external parties. The relations regarding such activities shall be regulated in an agreement. Such agreement shall set out the rights and obligations of the external parties involved in the certification service provision activities. Evrotrust uses subcontractors and service providers, such as specialized data centers, for reliable and secure colocation of server and network equipment, providers of cloud systems and services, providers of automated identification services, IT services and others. When working with subcontractors and providers, Evrotrust requires them to strictly follow its procedures, in accordance with this Policy and Practice.

1.6 QUALIFIED CERTIFICATES USAGE AND APPLICABILITY

Qualified electronic signature/stamp certificate for qualified electronic time-stamp or for website authenticity is issued by Evrotrust Technologies AD in its capacity of a qualified certification services provider and meets the requirements of usage and applicability set out in Regulation (EC) 910/2014.

The context of applicability of certificates may vary depending on the purpose for which they are used in the Republic of Bulgaria and other European countries, as in addition as a means of signing, they are also used in their role as a means of identification, establishing an encrypted TLS connection, encryption of data and others.

A description of the use and applicability of the Qualified Certificates is contained in the Policy for Providing Qualified Certificate for Qualified Electronic Signature / Seal.

1.7 PRACTICE MANAGEMENT IN QUALIFIED CERTIFICATE SERVICE PROVIDING

Each version of the Qualified Certification Service Practice is effective (current status) until the new version approval and publication. Each new version is developed by Evrotrust employees and is published after its approval by the Board of Directors.

Subscribers are required to comply only with the current version of the Practice at the time of use of Evrotrust services.

The Contact Person for management of the document "Practice in Providing Qualified Certification Services" by Evrotrust Technologies AD is the Executive Director of Evrotrust.

Further information can be obtained at the following address:

Evrotrust Technologies AD
Sofia, 1766
"Okolovrasten pat" 251G, Business center MM, floor 5
telephone, Fax: + 359 2 448 58 58
email: office@evrotrust.com

2. RESPONSIBILITY FOR PUBLICATION AND REPOSITORY

2.1 REPOSITORY

Evrotrust maintains a repository in which current and previous versions of electronic documents are located. Evrotrust manages and controls the company's website where it publishing all current versions of electronic documents and provides secure and continuous access to them by stakeholders. The certificates register is a database in which are published all the issued Evrotrust certificates, which are used during its activity, user certificates and certificate revocation lists. Regarding the repository, Evrotrust fulfils the following requirements:

- the certificates register contains PKI (Public Key Infrastructure Certificates) and Client Certificates available to subscribers, subjects and relying parties;
- ensures that all certificates published in the certificates register belong to the users or their authorized representatives;
- certificates shall be available to subject's consent has been obtained. If the subject is a device or system, the consent shall be obtained from the natural or legal person responsible for operating the device or system, instead of the subject;
- ensures that the certification bodies certificates belonging to Evrotrust and user certificates (subject to their prior approval) are published;
- publishes on its web site (https://www.evrotrust.com) the current "Qualified certification services policy", "Practice in providing qualified certification services", General Terms and Conditions, forms of documents for users and agreements between the parties as well as archived versions;
- gives access to information about certificates status by publishing CRL or by using OCSP protocol;

- All users and relying parties are provided with permanent access 24/7/365 to the information contained on the provider's web site at: https://www.evrotrust.com. Access to this information has no geographical restrictions;
- provides access to the certificates register for the certifying authorities, the Registration Authority, users and;
- publishes other information quickly and in accordance with the deadlines specified in this document;
- provides safe and controlled access to information in the certificates register.

All users have unrestricted access to all web site information.

2.2 INFORMATION PUBLISHED BY EVROTRUST

The Evrotrust website is available via address: https://www.evrotrust.com.

Access to the web site can be performed by HTTP/HTTPS protocol.

The information published by Evrotrust includes documents describing:

- Conditions and procedure for issuing an electronic certificate, including the rules for establishing the identity of the Certificate signatory;
- Security procedures for issuance and management of the certificates;
- Use of the certificates;
- Terms and conditions for use of the certificates, including requirements for private key storage;
- Conditions for access to a certificate and method of qualified certificate verification;
- Price for receipt and use of a certificate as well as prices for other services provided;
- Responsibility of Evrotrust and the Signatory/Creator of qualified electronic signature/seal;
- Terms and procedure by which the Signatory/Creator makes a request for cancellation of a qualified electronic signature/seal.
- Audit reports carried out by an authorized institution;
- Additional information, such as messages and notifications.

A part of the quoted information is contained in this document and in the Practices for providing other qualified certification services.

In addition to the documentation provided, Evrotrust also publishes in its repository:

- Its basic certificate (Evrotrust RSA Root CA);
- Operational Certificates of the Certification Authorities;
- Time-stamp Certificates;
- Certificates issued by Evrotrust;
- Certificate Revocation List (CRL) issued by Evrotrust.

2.3 FREQUENCY OF PUBLICATION

Evrotrust publishes information with the following frequency:

- "Qualified Certification Services Policy" and "Practice in Providing Qualified Certification Services " is subject to immediate publication upon each update;
- Operative certificates - each time a new certificate is issued;
- Updating of the certificates register of the issued certificates is done automatically and immediately after each newly issued valid certificate publication;
- Updating of the Certificate Revocation List (CRL) is done automatically but not more than 3 (three) hours or immediately after cancellation or blocking/renewal of a valid certificate. In all Certificate Revocation List (CRL), Evrotrust indicates the time for the next edition. The effective period of validity of the published current List is specified in it provided that an update is made;
- Additional information - for each event occurred

2.4 ACCESS TO PUBLICATIONS

Evrotrust offers access to publications that are available on its web site via HTTP/HTTPS-based access.

All web site information published by Evrotrust is publicly available. The access to the certificates register is also not limited by Evrotrust, except by the Signatory request and only in respect of his/her validly issued certificate.

The information published in the Evrotrust's web site is available on a permanent basis (24/7/365), except for events beyond Evrotrust's control and in the case of short-term temporary interruptions for regular check-up.

The Provider provides free access to all the basic and operational certificates of its active Certification Authorities as well as free access to all non-active ones for a period of at least 2 (two) years after the certificate expiry.

Communications between users and secure web pages of Evrotrust are implemented by using HTTPS protocol.

Evrotrust has taken measures, logical and physical mechanisms for protection against unauthorized addition, removal and change of the information published on the provider's web site.

Upon detecting violations of information, Evrotrust undertakes appropriate actions to restore the information integrity. If necessary, Evrotrust imposes legal sanctions, notifies the affected entities and compensates them for their losses.

3. IDENTITY IDENTIFICATION AND AUTHENTICATION

This part of the Practice introduces the general rules for user authentication applied by Evrotrust at issuing qualified certificates. Rules are based on certain types of information that is included in the certificates. This ensures that the information included is accurate and reliable at the time of the certificate issue. Data verification is mandatory at the user registration stage and at Evrotrust's request for all qualified authentication services.

The Registration Authority of the provider carries out the following identification procedures:

- ➢ accepts requests for issuing qualified certificates;
- ➢ performs a check to establish the identity of the Signatory, respectively the identity of the Creator and specific data about them with eligible means;
- ➢ approves after successful verification or rejects registered requests;
- ➢ notifies the Certification Authority to issue the required certificate.

Evrotrust, respectively the Registration Authority collects and receives the necessary identification information and verification of the Signatory/Creator's identity.

Evrotrust has developed a specialized system for remote video identification through a mobile application installed on the user's smart device. The same ensures user authentication in real time through automatic video identification based on received data and an image from the national date of base of identity documents or real-time videoconferencing from an operator on the basis of an identification document electronically provided and a specific methodology. The video identification system for natural persons used by Evrotrust has been certified for conformity to the requirements of Regulation (EU) № 910/2014 by the authority for verifying conformity, giving the same degree of security as personal appearance, pursuant to Art. 24, par. 4 of the Regulation (EU) № 910/2014

Automated remote identification of legal entities which will be entered in the issued qualified certificates as well as the legally representative power of the Signatory against them shall be established in real time by verification of the actual status and the entries in the commercial and other registers in which they are entered.

Where a verification cannot be made, the identification of the legal entities and the verification of the representative power shall be carried out on spot, on the basis of the documents submitted by an Evrotrust employee or a Registration Authority.

Evrotrust ensures that physical and legal persons are properly identified, that their identity is verified and that requests for qualified certificates issuance are fully, accurately duly verified and approved, including the full name/title and legal status of the natural person/legal person concerned and the relationship between the verified data and the natural/legal person.

Identification and identity verification of the Signatory/Creator are carried out prior to the issuance of a qualified certificate. These are performed by means of a remote identification system or by the personal appearance of the Owner/Creator or a person authorized by him before an Evrotrust employee or before a Registering Authority.

3.1 NAMES

Qualified certificates use all applicable names or other identifiers, including ASN.1 object identifiers. The name certificate requirements are as defined in the ITU-T X.509 or IETF RFC 5280 and ETSI EN 319 412 Recommendations. The names may be compliant with the Domain Name Service (DNS) described in RFC 2247.

The Registration Authorities shall verify and ensure that the names in the request for certificate issuance comply with the X.509 standard.

The “Subject" field on the certificate contains the Signatory/Creator’s/ Author’s name.

The name and other distinguishing signs of the Signatory/Creator’s in the corresponding fields for each type of certificate are in accordance with DN (Distinguished Name) formed according to X.500 and X.520 standard.

Evrotrust operative certificates contain in the "Subject" field and the "Issuer" field a DN attribute that forms its unique name.

A detailed specification of the certificates issued by Evrotrust is contained in the next sections of this document.

3.1.1 TYPES OF NAMES

The name requirements in the issued certificates are as specified in Recommendation ITU-T X.509 or IETF RFC 5280 and ETSI EN 319 412. The names may be in accordance with the Domain Name Service (DNS) described in RFC 2247. This way allows subscribers to use two types of names: DN and DNS at the same time.

In order to provide an easier way for electronic communication with the user, an alternative name (nickname) may also be used. The provider may issue a qualified certificate using a „nickname" to name the user only after the necessary identity information has been gathered for the same and it has been successfully identified. The name may also contain the user e-mail address which is to be in conformity to recommendation RFC 822.

3.1.2 MEANINGFUL NAMES REQUIRED

The names included in the Distinguished Name (DN) of the user have their meaning in Bulgarian or in other foreign language. The DN structure depends on the type of certificate and user. DN consists of the following areas (the descriptions are in conformity to RFC 3280 and X.520):

- Field C - an international abbreviation of the country name of (BG for Bulgaria),
- Field CN - full / frequent use of the natural person or organization name,
- Field GN - name of the natural person,
- Field SN – surname of the natural person,
- Field O - name of the institution the person represents,
- Field E - email address of the Signatory/Creator;
- Field SerialNumber - the natural person unique identifier,
- Other fields, which are detailed in the policies for the relevant qualified certificates profiles.

DN shall be verified by the Registration Authority operator and approved by the Certification Authority.

3.1.3 USER ANONYMITY

Evrotrust does not publish certificates and other credentials to ensure user data anonymity (e.g., CIN), unless the person expressly declares his/her willingness to do so.

3.1.4 RULES FOR DIFFERENT NAMES INTERPRETATION

Interpretation of fields provided in the certificates issued by Evrotrust are in conformity to the user profile certificates described below hereto.

The Common Name (CN) field contains the natural person name by which he/she is usually indicated in his/her activity in all Certificates where the Signatory is entered.

The unique name attribute (DN) also contains information about the personal identity or individuality of that person in the certificate, which includes a person on whose behalf the Signatory acts.

The name used in one user's certificate will never be used in another user's certificate.

3.1.5 UNIQUENESS OF THE NAMES

The "Subject" field in the certificate is formed by the Signatory/Creator information provided online or on paper by the person submitted the request or by an authorized representative when the initial request for issuing of certificate is registered and which is checked by the Registration Authority on the basis of documents, video identification and primary government registers verification.

Evrotrust ensures "DN" uniqueness of the Signatory/Creator in its domain by adding a requisite that guarantees such uniqueness.

Signatory/Creator with unique DN in the Evrotrust domain may have more than one issued valid qualified certificates.

Each issued certificate has an unique serial number ("SerialNumber") in the Evrotrust domain. The combination of „Issuer" and "SerialNumber" fields ensures the issued certificate uniqueness in the public domain.

3.1.6 NAMES VERIFICATIONS AND DISPUTES IN THIS REGARD

Names not owned by a requesting party cannot be used in its applications. In case of a doubt, the person is obliged to enclose documents proving names ownership.

It is beyond the care of Evrotrust to verify neither is the user entitled to use the name given in the registration request, nor can he act as arbitrator for disputes resolution. Evrotrust is not responsible when names used in the certificate violate foreign rights on a trade name, trademark, domain name, copyright, etc.

In the event of a dispute arising from the names used, Evrotrust shall reserve its right not to issue a certificate or terminate the contract for the maintenance of such unilaterally and without a notice.

Evrotrust shall not bear responsibility when names used by users in certificates violate foreign subjective rights.

3.2 INITIAL REGISTRATION

The user's initial registration is made when he/she first submits a request for registration to Evrotrust.

Registration includes procedures that allow data collection for his/her identity and the same to identify himself/herself before the user certificate is issued. These data conformation requires physical attendance in front of Evrotrust employee or its Registration Authority, notary or other authorized person confirming his/her identity/individuality. This procedure may be carried out remotely and, if possible, automated in the order stipulated above, by a remote identification system meeting the Regulation (EU) № 910/2014 requirements.

The user – physical person is obliged to submit to the Registration Authority representative the following information for unambiguous identification and verification of his/her identity:

- ➢ Names;
- ➢ Identity document- identity card, international passport or other identity document;
- ➢ National identification number, if any;
- ➢ Contact details - mobile phone, e-mail and address.

After the successful verification of the Signatory's identity, the authorized operator in the Registration Authority:

➢ offers a contract for qualified certification services signed on behalf of Evrotrust and stores all documents submitted to the contract;

➢ confirms the request for issuance and sends an electronic request for certificate issuance to the operating certification body of Evrotrust;

➢ records the issued certificate on a secure signature creation device (QSCD) and transmits it to the Signatory or the authorized person.

When using the remote identification system through a specially developed mobile application, the Signatory requests remote service provision by submitting an identity document and data from it, as well as mobile number and e-mail. In this case, the Signatory declares the contract conclusion of and the issuance of a qualified certificate for a qualified electronic signature and immediately automatic signing of the contract with Evrotrust.

A registration profile is maintained for every person in the Evrotrust systems.

3.2.1 PERSONAL KEY POSSESSION VERIFICATION

For issuance or continuation of a certificate, Evrotrust shall receive an electronic request in PKCS #10 format. The specification of this certificate request format requires that the request to be signed by the Signatory/Creator owning the private key.

Evrotrust verifies electronic signature/seal validity accompanying the request. The establishment of the validity of the electronic signature/seal placed is sufficient reason to be assumed that the Signatory/Creator has submitted an electronic request and possess a private key that is technically fit and corresponds to the public key contained in the request.

The key pair corresponding to the qualified certificate issued by Evrotrust shall be generated in an electronic signature/seal creation device.

Where remote issuance of a qualified electronic signature/seal certificate is requested, Evrotrust shall provide the Signatory/Creator with the service remotely by generating the key pair in a hardware crypto module meeting the requirements for a secure signature creation device. The private key is stored in encrypted form, using the Signatory's PIN code for encryption.

The access control to the private key is carried out only by the Signatory/Creator.

3.2.2 ESTABLISHING THE IDENTITY OF A LEGAL PERSON

Identity verification of legal persons (Creators) is carried out by a representative of the Registering Authority through a background check in the respective registers using a submitted UIC, BULSTAT or any other identifier of the person. Legal persons which cannot be subjected to an automated verification should submit:

- ➢ Judgment or other document certifying the legal person set up;
- ➢ Document certifying their good standing
- ➢ Unique national identifier.

After copying all required documents, with the consent of the person submitted the request, the copies remain in the Evrotrust's archive.

Where an authorized representative appears on behalf of a legal person, the authentication of the information contained in the documents submitted shall be carried out by:

- "Certification "True copy" and signature in handwriting on the documents before the Registration Authority employee in the event of the documents personal transfer;
- Notary certification of the documents, which are sent by mail to the Registration Authority;
- Signing of the attached electronic formats of the documents with a valid certificate for qualified electronic signature/seal;
- Review and confirmation using a specialized mobile or other application and after due identification of the representative and/or the legal person by an employee of Evrotrust.

The legal person authentication has two objectives. The first objective is to prove that the legal person exists during the request reviewing. The second objective is to prove that the representative person who applied for a certificate has been authorized to represent it by the legal person.

The Registration Authority employee can verify the registration through all available public services in conformity to the Bulgarian legislation.

When identifying persons requesting the issuance of certificates in compliance with the requirements of PSD2, Evrotrust verifies the specific features that the person provides and that shall be entered in the certificates to be issued based on authentic information kept by a National Competent Authority (NCA) (e.g. a public register). Where the relevant NCA has laid down rules for the verification of the relevant features, Evrotrust complies with and applies them.

If the subject is a device or system operated by or on behalf of a legal person, or other organizational entity identified in association with a legal person, shall be checked against a duly man dated subscriber either directly, by physical presence of a person, or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

3.2.3 ESTABLISHING THE IDENTITY OF A NATURAL PERSON

The identification and verification of the identity of the natural person (Signatory) is carried out by a representative of the Registration Authority. Identification can also be done automated by remote verification.

An identity document is required to be produced for identifying and verifying the identity of the natural person.

The natural person who requests issuance or management of a qualified certificate shall complete and transmit to Evrotrust documents in conformity to the provider policy for the issuance and management of qualified certificates. The personal data can include mobile phone number, email address, home address, etc. The natural person confirms data authenticity by:

- Signature in handwriting on the documents before the Registration Authority employee, in the case of documents personal transfer;
- Notary certification of the documents, which are sent by mail to the Registration Authority;
- Signing of the attached electronic documents by a valid certificate for a qualified electronic signature within the meaning of the Regulation (EU) № 910/2014;

Evrotrust can establish the natural person identity in the order stipulated above by using a specialized mobile or other application and after an automated identification of the natural person or by Evrotrust employee.

When using the Evrotrust mobile application, physical identification is performed through an automated video identification system by checking a scanned identity document and obtaining data on its validity from a national database of Bulgarian identity documents as well as biometric analysis of the face with photo material obtained from the national database. In the event of a failure, identification is performed by an operator using a special methodology through videoconference. The verification of the representative power of a natural person against the legal entity is carried out by checking the data for the entries in the respective registers with the Registry Agency.

Evrotrust performs verification of the information authenticity in the completed documents by all legally permitted means in the respective public registers.

A list of required documents for a natural person for issuing and managing of a qualified certificate is maintained on the Evrotrust web site.

3.2.4 ESTABLISHMENT OF THE IDENTITY OF A NATURAL PERSON, AUTHORIZED REPRESENTATIVE OF A LEGAL ENTITY

For the issuance of a qualified certificate to an individual (Holder), which is authorized by a legal person, the authorized representative have to appear in front of the Registration Authority. Validation of the information contained in the submitted documents is done by:

- "True to the original" certification and a handwritten signature on the documents in front of the employee of the Registration Authority in the case of personal transmission of the documents;

- Notary certification of the documents, which are sent by mail to the Registration Authority;
- Signing of the attached electronic formats of the documents with a valid certificate for qualified electronic signature / seal;
- review and confirmation by using a specialized mobile or other application and after proper identification of the representative and / or legal entity by an employee of Evrotrust as well as by checking the registrations of the representative authority in the official registers (to the Registry Agency).

The verification of the identity of a legal entity seeks to prove that during the examination of the application the legal person exists and that the representative who applies for a qualified certificate has the power to request the issue.

3.2.5 SPECIAL ATTRIBUTES

The Provider may include special attributes in the issued certificate associated with the Signatory if the certificate is issued for a particular purpose under the relevant policy.

This information is subject to verification by the Registration Authority.

Evrotrust issues, at the request of a person for identification purposes before a relying party Evrotrust Qualified Natural Person Attribute Certificate for QES" with a short term of validity containing all text requisites of the identity document as far as they are provided at the time of his/her registration as an user by the person.

3.2.6 UNCONFIRMED INFORMATION

Any information beyond the compulsory verified is unconfirmed information.

The Provider may include in the issued certificate and unconfirmed information for the Signatory/Creator that is not subject to verification by the Registration Authority. In this case, Evrotrust shall bear no responsibility for this information.

3.2.7 CERTIFICATION AUTHORITY ACTIONS

Upon successful identification and verification of the conditions for issuance or management of a qualified certificate by the Registration Authority, a Registration Authority representative confirms the data to the Certification Authority. The Certification Authority shall immediately publish the issued certificate in the certificates register, respectively the maintenance information in the Certificate Revocation List (CRL).

In Evrotrust, only the Operational Certification Authority that has issued a qualified electronic signature / seal certificate may terminate this certificate.

3.2.8 DOMAIN LICENSE VERIFICATION

When issuing qualified website authentication certificates, Evrotrust verifies if domain registration and Signatoryship in the public WhoIs databases correspond to the person requesting the certificate. Where no such public information is available, users themselves provide the information necessary to prove domain Signatoryship, subject to verification by Evrotrust.

3.2.9 CRITERIA FOR CONFORMITY

Qualified certificates issued by Evrotrust meet the requirements of Regulation (EU) 910/2014 and are recognized in the European Union. Given the cross-border interoperability of the qualified electronic signatures and seals formats introduced by the Regulation (EU) № 910/2014, qualified certificates do not exceed the mandatory requirements of the Regulation (EU) № 910/2014. At national level, qualified certificates include specific data such as Civil Identification Number and other specific data at the user's request, but Evrotrust ensures that they do not hinder cross-border interoperability and recognition of qualified certificates and electronic signatures/seals in the European Community.

3.3 IDENTIFICATION AND IDENTITY VERIFICATION UNDER A PROCEDURE FOR A QUALIFIED CERTIFICATE RENEWAL

Evrotrust may renew a validly qualified certificate which has not been terminated within its term of validity generating a new key pair ("Re-key").

Evrotrust does not maintain the option for Renewal with preservation of the existing key pair (Renewal) or with preservation of the serial number.

Evrotrust renews current Signatory/Creator certificates with a new key pair (Re-key) only if there have been no changes in the verified information. Renewed certificates contain new serial numbers, new public keys, new validity periods and new electronic signatures/seals of the Certification Body, whereby the verified information therein remains the same.

Upon renewal, the current qualified certificate shall not be terminated and shall remain valid within its period of validity.

Existing evidences can be re-used to validate the identity depending on applicable legislation and whether the evidence remains valid given the time elapsed.

His/her personal attendance is not required before the Evrotrust Registration Authority for identification and identity verification of Signatory/Creator of the qualified certificate, which is renewed,

In the event of changes of the information about the Signatory/Creator of qualified certificate, the current certificate is not renewed. The provider issues a new qualified certificate following the initial identification and identity verification and terminates the current qualified certificate immediately.

The Provider complies with the following time limits and identification requirements when renewing a qualified electronic certificate:

Period	**Renewal**	**Requirements**
Up to 30 days before the expiry of the validity of the qualified certificate, which has not been terminated and which has no change in the information certified in it	➢ by Re-key	➢ There is no change in the certificate "DN" ➢ The renewal request can be made remotely
Up to 30 days after the expiry of the validity of the qualified certificate, which has not been terminated and that there is no change in the information certified in it	➢ by Re-key	➢ There is no change in the certificate "DN" ➢ The renewal request can be made on place (in the Registration Authority)
More than 30 days after the expiry of the qualified certificate	It is not renewed	

In the event of remote issuance and renewal of qualified certificates through a mobile application, the renewal is always "Re-key" and a new certificate shall be mandatory issued. In this case, identity and identification checks are not carried out but identity authentication checks are performed.

With a view to PSD2 compliance, when renewing certificates that contain any information, subject to PSD2 requirements, Evrotrust verifies it again and in doing so may request it again from the relevant NCA. Where the relevant NCA has laid down rules for the verification of the relevant features, Evrotrust complies with and applies them.

3.4 IDENTIFICATION AND VERIFICATION OF IDENTITY IN THE EVENT OF A QUALIFIED CERTIFICATE SUSPENSION

Suspension of validity of qualified certificates is established Evrotrust operational practice and differs from termination in that it leads to the temporary termination of the certification power of a certificate. For legal reasons, Evrotrust always clearly notes the status of the certificates validity suspension.

Evrotrust is obliged to suspend the operation of a valid certificate through the Registration Authority upon a request for suspension. The time in the systems related to stopping and terminating certificates is synchronized to UTC at least every 24 hours.

The Provider, through the Registration Authority, does not identify and verify the identity of the Signatory's/Creator's and immediately stops the certificate operation.

When a remote qualification certificate is issued, it can be suspended by the mobile application immediately by the user, through the functionality provided.

3.5 IDENTIFICATION AND VERIFICATION OF IDENTITY IN THE EVENT OF A QUALIFIED CERTIFICATE TERMINATION

When Evrotrust terminates the qualified certificate, it shall reflect this in the databases it maintains dully but no later than 24 hours after the request is received. Cancellation becomes valid as soon as it is published.

Evrotrust terminates the validity of a certificate only after successful identification and identity verification of the Signatory/Creator and a specified reason for termination. Otherwise, the certificate is renewed.

Upon termination through the mobile application, identity and individuality verifications are not performed due to the Signatory's access to the appropriate functionality.

Evrotrust provides each trusting party with information on the termination of the qualified certificates operation issued by it, upon request. This information is made available at any time and even after the validity of the certificate.

3.6 IDENTIFICATION AND VERIFICATION OF IDENTITY AFTER TERMINATION OF A QUALIFIED CERTIFICATE

Policy and practice of providing qualified certification services of Evrotrust does not allow a qualified certificate renewal after its termination.

The Signatory/Creator of a terminated certificate may request the issuance of a new one.

The Provider, through the Registration Authority, performs initial identification and identity verification of the Signatory/Creator if he/she requests a new certificate. This verification is is not performed if the user requests issuance of a new qualified certificate from the mobile application where he/she has an active account.

4. OPERATIONAL REQUIREMENTS

Evrotrust, through the Registration Authority, within the framework of the concluded Qualified Certification Services Agreement, provides the following operating procedures for qualified certification services applicable to qualified electronic signatures/seals:

- registering of a request for a qualified certificate;
- handling of a request for a qualified certificate;
- issuing of a qualified certificate;
- transmitting of the issued qualified certificate;
- use of the pair key and a qualified certificate;
- renewing of a qualified certificate;
- suspension/renewal of a qualified certificate;
- termination of a qualified certificate;
- qualified certificate status.

The Provider, through the Registration Authority, allows the Signatory/Creator to terminate the Qualified Certification Services Agreement between them.

The time in the systems associated with certificates suspension and termination is synchronized to UTC at least once per every 24 hours.

4.1 SUBMISSION OF A REQUEST FOR QUALIFIED CERTIFICATE ISSUANCE

Submission of a request for qualified certificate is a process where the user submits a request for issuance of a qualified certificate to the Registration Authority of Evrotrust, in writing or in electronic form, under the policy of issuing the relevant certificate.

The request may be made by the Signatory/Creator or an authorized representative of the Author.

The user registers a request for a qualified certificate issuance online or through an operator at the Registration Authority of Evrotrust.

In online mode, requests are submitted through network protocols such as HTTP/HTTPS, S/MIME or TCP/IP.

A request for a qualified certificate can also be submitted via the Evrotrust mobile application. In this case, the above requirements do not apply.

4.1.1 PERSONS SUBMITTING A REQUEST FOR A QUALIFIED CERTIFICATE ISSUANCE

Any person belonging to one of the following categories of persons may apply for a qualified certificate:

- a natural person who will use a qualified certificate as a consumer,
- an authorized representative of a legal person;
- a Evrotrust employee, authorized with functions to the Evrotrust Certification Authority;
- an authorized person to the Registration Authority, whether it is an external organization or an organizational unit to the Evrotrust infrastructure.

4.1.2 PROCESSING OF THE REQUEST FOR A QUALIFIED CERTIFICATE ISSUANCE

4.1.2.1 USER CERTIFICATES

By signing of the Certification Services Agreement all users of qualified certificates shall accept the obligations and warranties set forth therein as well as the Qualified Services Policy and this Practice. Each user of a qualified certificate undergoes a registration process that includes the following steps:

- submitting of a request for a qualified certificate that contains true and accurate information. The request may include additional, unverifiable information, a part of which is certified, and another part facilitates the contact between Evrotrust and the Signatory/Creator;
- generating cryptographic pair key by Evrotrust or the user performs it himself. The cryptographic pair key for Qualified QES/QES seal Certificates shall be generated on a secure signature/seal creation device meeting the security level requirements defined in the Regulation

(EU) № 910/2014;

➢ the electronic format of the request for issuance of a qualified certificate with the information to be included in the certificate is a structure signed with the private key of the generated pair key at the secure signature/seal creation device unless the request is made remotely through Evrotrust mobile application;

➢ where necessary, the Registration Authority submits to the Signatory/Creator or a person authorized by him/her in protected form information/code for access to the private key at the secure signature/seal creation device;

➢ in the case of a remote generation of a pair key by the user, the user shall provide the public key to Evrotrust through the registration authority and prove ownership of the corresponding private key corresponding to the public key;

➢ on the basis of the approved requests for issuance and management of a qualified certificate, the contract with Evrotrust is signed.

4.1.2.2 CERTIFYING AUTHORITY AND REGISTRATION AUTHORITY CERTIFICATES

Registration authorities providing qualified services that are not in Evrotrust's organizational structure (external Registration authorities) are required prior to performing this activity to enter into an appropriate contract with Evrotrust. In the agreement, besides the rights and obligations of both parties, information should also be included on the identity of the persons participating in the Registration Authority and their authorization to represent both parties during the contract execution. The persons authorized to carry out this activity shall define the certificates type and designation before issuing them.

Certification Authority keys and certificates can only be generated during a key generation ceremony involving only persons authorized by Evrotrust.

4.1.2.3 REQUEST FOR REGISTRATION OF USERS OF QUALIFIED CERTIFICATION SERVICES

The request for registration of users of qualified certification services is submitted at the Registration Authority by physical, legal or authorized persons and includes the following information:

➢ full name of Signatory/Creator or of authorized person;

➢ evidence of the representative power of the Signatory over the Author and of the

Authorized Person of the Author ;

- identifiers: UIC (Unique Identification Code), etc.;
- the person's postal address (country, district, zip code, town or village, building number, street or neighbourhood name, fax number);
- email address;
- type of the qualified certificate requested, taking into account its designation;
- identifier of the authentication policy on the basis of which the certificate is issued;
- presence of a private key corresponding to a public key;
- public key;
- additional information requested to be included in the certificate as well as admissible unconfirmed one;
- signing of a Qualified Certification Services Agreement and agreeing to the terms and conditions of the Policy and Practice for providing qualified certification services by Evrotrust.

Depending on the certificate content and its type, some of the data listed above may be absent.

If the cryptographic key pair is generated by the Signatory/Creator, the Registration Authority shall check the submitted electronic registration request and the security level requirements of the secure signature creation device

After successful identification, verification of the identity of the person applying for a qualified certificate and upon receipt of the Registration Authority conformation, the registration request shall be sent to the Certification Authority for the certificate issuance.

4.1.2.4 RENEWAL OF A QUALIFIED CERTIFICATE, GENERATION OF A NEW KEY PAIR AND CHANGE OF A QUALIFIED CERTIFICATE

The Signatory/Creator or the Authorized Person may request the qualified certificate renewal, subject to the time limits, renewal requirements and conditions.

Qualified certificate renewal keeps the Signatory's/Creator's or the Authorized Person's information from the current certificate where the validity period and the serial number are changed in the renewed certificate.

Qualified certificates which have not been terminated during their validity period may be renewed through the generation of a new key pair (Re-key). Evrotrust does not maintain the option for Renewal with preservation of the existing key pair (Renewal) or with preservation of the serial number.

The qualified certificate renewal is preceded by the registration of a renewal request to the Registration Authority or online.

When the qualified certificate has expired and the renewal request is within the specified time limits and the renewal identification requirements, the Signatory/Creator or the Authorized Person shall visit Evrotrust's Registration Authority or to perform remote identification.

The Signatory/Creator or the Authorized Person may repeatedly renew a qualified electronic signature/seal certificate.

The Provider does not allow the use of a key pair for electronic signature/seal for a period longer than 3 (three) years.

The Registration Authority is to renew a qualified electronic signature/seal certificate by Re-key under the following conditions:

- the certificate is not terminated during the period of its validity;
- the Signatory/Creator or the authorized person declares that there is no change in the certified information in his/her current certificate;
- a request for renewal of a qualified certificate is made up to 30 days before or after the expiry of the period of validity of the certificate;
- strictly performs the user's identification and verification and the time limits specified at renewal;

In all cases where there is a change in the certified information for the Signatory/Creator or the authorized person of the current certificate, the latter is not renewable and Evrotrust issues a new qualified certificate.

Request for renewal of a qualified certificate shall contain at least the following:

- the unique name of the Signatory/Creator or the authorized person;
- qualified certificate type/ designation;
- Identifier of the authentication policy on the basis of which the certificate is issued;

Some or all of the data contained in the request for renewal of a qualified certificate may be authenticated by affixing an electronic signature/seal on condition that the subscriber holds a valid private key for creating signature/seal at the time.

The provider does not allow a change in the profile of the electronic signature/seal certificates.

Renewal of a qualified certificate requested remotely through the Evrotrust mobile application is not renewed. A new certificate is issued after it expires. In this case, additional identification is not carried out, but only verification of authenticity of the identity data.

4.1.2.5 REQUEST FOR SUSPENSION AND TERMINATION OF CERTIFICATE

A request for termination of a qualified certificate is submitted by the Signatory/Creator or the authorized person on site at the Registration Authority or electronically.

At the time of termination of a qualified certificate, the Registration Authority informs the user of this fact (for example, by e-mail).

Evrotrust terminates a certificate issued by it in case of:

- death or imprisonment of the Signatory/Creator by termination of the representative power of the Creator;
- termination of the representative power of the Signatory towards the Creator;
- establishing false data when issuing the certificate;
- information subsequently became false;
- upon a change of already certified information of the Signatory/Creator;
- compromising of the private key;
- delay in payment of the due remuneration;
- request for termination by the Signatory/Creator , once the Provider has ascertained Author's identity and the representative power. When a suspension or termination of a qualified certificate is requested through the Evrotrust mobile application, identity verification is not performed.

The provider shall immediately terminate the operation of a valid certificate issued in each of the above circumstances.

The provider shall terminate the issued certificates if it ceases its activity without transferring it to another provider. In this case, it shall notify its users and terminates the certificates with one month's notice. Within one month of being notified, Evrotrust shall reimburse the amount paid to the users in an amount consistent with the remaining period of the Qualified Certification Service Agreement. When a qualified certificate is requested through the Evrotrust mobile application, the subscriber's subscription terminates from the moment the next renewal period occurs.

The Provider may suspend and terminate an Infrastructure Certification Authority if there are reasonable grounds for compromising the Authority’s private key.

Upon termination of the certificate of the operational Certification Authority for issuance and maintenance of qualified certificates for electronic signature/seal, the validity of all issued and valid certificates by it shall be terminated.

Only the operational Certification Authority that has issued a qualified electronic signature/seal certificate may terminate this certificate.

If the termination results from an operator error or a consequence of compromising of an Evrotrust operational private key, the Provider will issue an equivalent user certificate at its own expense.

Termination and suspension management services are available 24 hours a day, 7 days a week.

In the event of a system failure, services or other factors beyond the control of the Certification Authority, Evrotrust shall make every effort to ensure that the service is available within 3 (three) hours.

The time in the systems associated with suspending and terminating certificates is synchronized to UTC at least once every 24 hours.

Concerning the PSD2 compliance, requests for cessation or termination of certificates may also be submitted by the NCA for issued certificates containing an authorization number of the payment institution of Payment service provider (Payment Service Provider/PSP) registered with the same NCA. Furthermore, the relevant NCA shall specify the serial number of the certificate at issue, as well as the reason for cessation or termination. The possible reasons for termination are:

- Terminated PSP authorization;
- A change in the payment institution's authorization number PSP;
- A change in the name or identifier of the an NCA;
- Termination of one or more of the roles certified with the issued certificate. The assumption of a new role by a PSP is not a reason to terminate an issued certificate;
- The termination is required by law;
- Other reasons.

If a NCA holds specific information under PDS2 and notifies Evrotrust that this information has been modified and that it concerns the validity of a certificate issued by Evrotrust, Evrotrust shall verify the information in question, regardless of the content and format thereof, without being obliged to do so within 24 hours.

Evrotrust verifies the authenticity and the veracity of the information and the requests extended by the NCA and, where necessary, may perform or refuse the performance thereof, without being obliged to provide any reasons for the acceptance or refusal thereof.

4.2 REQUEST PROCESSING

Evrotrust accepts requests for qualified certification services submitted individually. Requests can be submitted online via a publicly accessible web-based application and on site at the Registration Authority. In case the documents are sent by post, a notary certification of the signatures is required. Requests can also be accepted through the Evrotrust mobile application.

Online submission via a publicly accessible web-based application is available through the provider's website at: https://www.evrotrust.com. The user who has visited the corresponding section of the site completes (in accordance with the instructions on this site) a corresponding application form and sends it to the Registration Authority online. Requests for qualified certification services are processed by an Evrotrust employee.

When a request is submitted to a Registration Authority, a Signatory/Creator or an authorized person attendance is required. In case of authorization, documents proving authenticity are required.

When a request is submitted through the Evrotrust mobile application, it is generated automatically in a user-friendly dialogue mode.

4.2.1 IDENTIFICATION AND VERIFICATION OF IDENTITY

Identification and identity verification activities of Evrotrust users are carried out by the Registration Authority in accordance with the terms and conditions set out in this document.

4.2.2 ACCEPTANCE OR REJECTION OF A REQUEST

4.2.2.1 PROCESSING OF A REQUEST BY THE REGISTERING AUTHORITY

Any request submitted electronically or on a hard copy to the Registration Authority is processed as follows:

- ➢ The Registration Authority receives the request from the Signatory/Creator or the authorized person (in a hard copy or in an electronic format);
- ➢ The Registration Authority checks if the person has paid a fee for reviewing a qualified certificate request, provided that the payment is provided in the Evrotrust price list. In the

absence of such a fee, the request shall be rejected;

- The Registration Authority verifies the data specified in the request, such as the person's personal data, and verifications for ownership of a private key;
- In case of a positive verification, the Registration Authority confirms the request;
- If the original request contains incorrect information, it is rejected or corrected;
- A certificate is issued as a result of the confirmation;
- The Registration Authority may also verify other data not specified in the request but required by Evrotrust.

In the event of submitting the request through a mobile application, the above procedures do not apply. In this case, a verified identity of the person and identification s verified - automatically or by an operator. In the event of technological availability, automated verification is carried out in the national database of identity documents or population registers. If the verifications are satisfactory, Evrotrust generates the key pair remotely, in its hardware crypto module, encrypts the user private key with its PIN and issues the qualified certificate.

4.2.2.2 REQUEST TO THE CERTIFYING AUTHORITY FOR ISSUE OF A QUALIFIED CERTIFICATE

Evrotrust may refuse to issue a qualified certificate to any person without any liability or responsibility if the user indicates incorrect data in the certificate request.

Evrotrust may refuse to issue a qualified certificate:

- if the user cannot prove his/her rights on the proposed DN;
- in case of a doubt that the user falsifies data or indicates incorrect data;
- if the user engages significant resources from Evrotrust to handle more requests than needed;
- if the user does not make a payment for issue of a certificate, provided that the payment is provided in the Evrotrust price list;
- if other important reasons not mentioned above exist.

Candidates whose requests are rejected may subsequently reapply for a qualified certificate.

4.2.3 WAITING FOR A QUALIFIED CERTIFICATE ISSUE

The Registration Authority of Evrotrust immediately, in the presence of the user -

Signatory/Creator or a person authorized by him/her, performs all the functions of checking the request for the issuance of a qualified certificate.

The Evrotrust Certification Body issues a Qualified Certificate immediately upon validation of the electronic request for issuance by the Registration Authority.

Evrotrust ensures that upon receipt of a request for issuance or management of a certificate, the Registration Authority will examine the request and issue the certificate immediately and, in special occasions, no longer than 3 days from the day of submitting.

This period depends mainly on the type of qualified certificate, the completeness of the request submitted and the technological time for coordination of the service between the administrative structures of the provider and the time of communication between Evrotrust and the user.

When a qualified certificate is issued through the Evrotrust mobile application, the above procedures do not apply and no waiting is done. In this case, the certificate shall be issued immediately in the presence of successful identification and identity verifications.

4.3 QUALIFIED CERTIFICATE ISSUE

4.3.1 PROCESSING

Upon receipt of a qualified certificate request and its processing, the certificate is issued by the Certification Authority.

All certificates are issued in real time. The issuing procedure is as follows:

- ➢ any request for issue of a qualified certificate is recorded and verified by the Registration Authority;
- ➢ only persons performing trusted roles have access to the operative actions the Registration Authority. Account usage protects multi-level operations and allows secure processing of a qualified certificate request, including the creation of an appropriately formatted certificate request by the Certification Authority;
- ➢ the processed and formatted certificate request is sent to the server for issuing a qualified certificate according to the selected profile;
- ➢ the Certification Authority generates the requested certificate, signs it with the electronic signature of Evrotrust and immediately publishes it in its Public Register;
- ➢ The Certification Authority prepares a response containing the issued certificate and provides it to the User;

- Evrotrust not issue certificates whose lifetime exceeds that of the CA.

By remote requesting of a certificate through the Evrotrust mobile application, the same is issued in real time immediately, within the user registration session.

4.3.2 PROVISION OF INFORMATION

An Authorized Representative of the Registration Authority of Evrotrust shall immediately notify the Signatory/Creator or the person authorized by the Author for the issued and published certificate.

An Authorized Representative of the Registration Authority of Evrotrust shall send to the Signatory/Creator an electronic notice by email with information about the Signatory's name, the type of the electronic signature/seal issued, the unique serial number of the qualified certificate and its period of validity, except where an e-mail address is missing.

The provider shall deliver the issued certificate to the Signatory/Creator, respectively to the person authorized by it, through the Registration Authority.

In case, when TSP managing the private key on behalf of the user, the complete and accurate certificate is available for use by the subscriber or subject or, if needed. The certificate does not need to be available for use immediately upon generation.

An Authorized Registration Authority operator enters the certificate of secure signature creation device where the pair of cryptographic keys for that certificate has been generated.

These rules also apply to the remote issuance of qualified certificates through the Evrotrust mobile application. In this case, the Signatory's/Creator's notifying is done by sending a message to the mobile application itself.

4.4 ACCEPTANCE OF A QUALIFIED CERTIFICATE

4.4.1 CONFIRMATION OF ACCEPTANCE OF A QUALIFIED CERTIFICATE

Upon receipt of a qualified certificate, the user is required to verify its content regarding the accuracy of the data and the availability of a public key corresponding to the private key it owns. If false information is entered in the certificate, the certificate must be terminated immediately.

If the Signature Owner/Author objects that the issued qualified certificate contains errors or omissions within 3 (three) days of its publication in the Register, Evrotrust shall remove them by issuing a new certificate without payment of remuneration unless they are due to the provision of false data. In the absence of an objection, the content of the certificate shall be deemed to have been accepted.

The rules in this section apply both to the issue of a certificate and to the renewal of a certificate.

Following the procedure for the acceptance of a qualified certificate, it is assumed that the user has been familiar with the certificate issuance procedures described in this document.

By accepting the qualified certificate, the user accepts the Practice and Policy for the provision of Qualified Certification Services.

4.4.2 PUBLICATION OF A QUALIFIED CERTIFICATE

Each issued and accepted certificate shall be published immediately in the certificates register of Evrotrust.

4.4.3 INFORMATION FOR OTHER PARTIES

Following the publication of the certificate issued in the certificates register, it becomes available to all interested parties after the execution of the applicable access procedures.

4.5 USE OF THE QUALIFIED CERTIFICATE AND THE KEY PAIR

4.5.1 BY THE SIGNATURE OWNERS/AUTHORS

The Signature Owners/Authors must use the private keys and qualified certificates:

- ➢ in accordance with their intended use as specified in this Practice and in accordance with the limitations and purposes of use listed in the Annex itself, and in relation to the attributes of the certificate itself;
- ➢ in accordance with the supplementary agreement between the user and Evrotrust;
- ➢ only within the period of their validity;
- ➢ when the certificate is suspended, the user must not use the private key to create an electronic signature/seal.

The Signature Owner/Author is not allowed to provide his or her private key to third parties, nor to provide the medium to which it is customized or the means of identification. The Signature Owner/Author shall be responsible for the privacy of the private key.

4.5.2 BY THE RELYING PARTIES

The relying parties, including operators in the Registration Authority, must exercise due care when using the public keys and their respective certificates:

- in accordance with their intended use and limitations of use specified in this Practice, and in relation to the attributes of the certificate itself;
- only after checking their status and verification of the electronic signature of the Certification Authority that has issued the certificate;
- until the termination of the certificate;
- when the certificate is suspended, the relying party should not accept the public key.

4.6 RENEWAL OF A QUALIFIED CERTIFICATE

Renewal of a qualified certificate means replacing a valid certificate with a new one without changing the existing information in it except a new serial number, new key pairs, new validity period and new electronic signature/seal from the Registration Authority.

It must be preceded by the submission of a renewal request in an appropriate form accepted and approved by an operator in a Registration Authority, verified identity and correctness of the submitted application.

4.7 ISSUANCE OF A QUALIFIED CERTIFICATE BY GENERATING A NEW KEY PAIR

A new key pair is generated by Evrotrust in cases where an already registered user requests a new key pair generation or a new user requests a key pair generation. The new key pair generation is accompanied by the issuance of a new qualified certificate confirming the ownership of the newly created key pair.

Issuance and renewal of Re-key should be interpreted in the following way:

- the issuance of a new key pair is not associated with any valid certificates and is used by users to obtain a certificate of any kind;
- refers to a specifically valid certificate specified in the request. As a consequence, the new certificate includes the same content and the differences are: a new serial number, a new public key, a new expiration date and a new electronic signature/seal from the Registration Authority.

Evrotrust shall inform their users in advance by email at least 14 days before the expiration of the validity of the issued certificate when it is possible.

The procedure for issuance of a qualified certificate with the generation of a new key pair may also be applied to the Certification Authority and to the Registration Authority.

The procedures under this item shall not be applied to qualified certificates issued remotely through the Evrotrust mobile application.

4.7.1 CIRCUMSTANCES UNDER WHICH A QUALIFIED CERTIFICATE IS ISSUED BY GENERATING A NEW KEY PAIR (RE-KEY)

A user's request for renewal of qualified certificate by generating new key pairs submitted to Evrotrust may be applied in case:

- the user is the same;
- the certificate is valid at the time of submission of the request and has not been cancelled;
- the user requires an additional certificate of the same type or of a different type, but only under the policy for authentication of a valid qualified certificate;

4.7.2 WHO MAY REQUEST A KEY PAIR UPDATE?

The request for issuance of a qualified certificate by generating a new key pair shall be submitted solely by the Signature Owner/Author or a person authorized by him/her.

4.7.3 KEY PAIR UPDATE AND REQUEST PROCESSING

The issuance of qualified certificates by generating new key pairs for electronic signatures/seals is preceded by the registration of a renewal request with the Registering Authority of Evrotrust.

The request for renewal of a qualified certificate submitted electronically shall be certified by an electronic signature/seal corresponding to the valid certificate of the Signature Owner/ Author or a person authorized by him/her.

In case the renewal certificate has expired, the Signature Owner/Author or a person authorized by him/her has to visit the Evrotrust Registration Authority or to perform remote identification. An authorized operator of the Registration Authority strictly follows the requirements for identification and authentication as well as the renewal conditions.

Upon successful identification and verification of the renewal conditions, the Registration Authority confirms the renewal request to the Evrotrust Operational Certification Authority.

After successful electronic authentication of the Registration Authority through the authorized operator, the Operational Certification Authority executes the confirmed request for renewal of the certificate.

Upon unsuccessful identification and verification of the renewal conditions, the Registration Authority rejects the request for renewal of the certificate and notifies the user of the rejection. In this case, the user with a rejected renewal request may request the issuance of a new certificate.

A renewal under this item shall not be applied to qualified certificates issued remotely through the Evrotrust mobile application.

4.7.4 INFORMATION FOR THE SIGNATURE OWNER/AUTHOR

An authorized representative of the Evrotrust Registration Authority shall immediately notify the Signature Owner/Author or a person authorized by him/her of the renewed and published certificate.

In cases where the request is submitted electronically via a publicly available web-based application, Evrotrust sends electronically (by e-mail) information about the new qualified certificate: the name of the user, the type of the qualified certificate, the unique serial number and the period of validity of the renewed certificate. The e-mail address from which the new qualified certificate can be downloaded is also sent.

When the request is submitted on-site at the Registration Authority, the Signature Owner/Author or a person authorized by him/her receives the renewed qualified certificate by an authorized operator of the Registration Authority. The operator records it on a device for electronic signature/seal creation in which the cryptographic key pair for the qualified certificate has been generated.

4.7.5 CONFIRMATION OF ACCEPTANCE OF A NEW CERTIFICATE

Upon receiving a new qualified certificate, the Signature Owner/Author shall be obliged to comply with the requirements above.

4.7.6 PUBLICATION OF A NEW QUALIFIED CERTIFICATE

After the immediate publication of the issued certificate in the certificates register, it becomes available without restriction to all relying parties upon completion of the relevant procedures for access to it.

4.7.7 INFORMATION FOR RELYING PARTIES

Following the immediate publication of the certificate issued in the Public Register of Issued Certificates, it becomes available to all interested parties.

4.8 CHANGE IN THE QUALIFIED CERTIFICATE

4.8.1 CIRCUMSTANCES FOR CHANGE IN THE QUALIFIED CERTIFICATE

A change in the qualified certificate means a change in the content of data in the already issued and published qualified electronic signature/seal certificate. Upon change in a qualified certificate, a new key pair is required to be generated.

The change shall be treated in the same way as the issuance of a new qualified certificate.

Evrotrust does not allow a change in the profile of the qualified electronic signature/seal certificates.

A change shall not be allowed to qualified certificates issued remotely through the Evrotrust mobile application. They shall be terminated and new ones shall be issued in their place.

4.8.2 WHO MAY REQUEST A CHANGE IN A QUALIFIED CERTIFICATE?

An Signatory/Creator, a person authorized thereby, another person associated therewith, or a person that is a source or is related to the data in the certificate, may request a change of the qualified certificate, provided that the requirements, terms and conditions stipulated herein are met.

4.8.3 PROCESSING OF THE REQUEST

The change of a qualified electronic signature/seal certificate shall be preceded by the submission of a request for a change by the Signature Owner/Author or a person authorized by him/her at the Evrotrust Registration Authority.

The request for a change by electronic application shall be certified by an electronic signature/seal of the Signature Owner/ Author corresponding to a valid qualified certificate.

In case the certificate being changed has expired, the Signature Owner/Author or a person authorized by him/her has to visit the Evrotrust Registration Authority or to perform remote identification. The Registration Authority strictly follows the requirements for identification and authentication as well as the conditions for a change of a qualified certificate.

Upon successful identification and verification of the conditions for a change, the Registration Authority confirms the request to the Evrotrust Operational Certification Authority.

After successful electronic authentication of the authorized operator of the Registration Authority to the Operational Certification Authority, the latter executes the confirmed request for a change of the qualified certificate.

Upon unsuccessful identification and verification of the conditions for a change, the Registration Authority rejects the request and immediately notifies the user of the reason. In this case, the user with a rejected request for a change may request the issuance of a new qualified electronic signature/seal certificate.

4.8.4 INFORMATION FOR THE USER

An authorized officer of the Evrotrust Registration Authority shall immediately notify the Signature Owner/Author or a person authorized by him/her of the changed and published qualified certificate.

The Provider sends to the Signature Owner/Author an electronic notice (e-mail) with the name of the Signature Owner/Author, the type of the qualified electronic signature/seal certificate, the unique serial number and the term of validity of the changed certificate. The user also receives an electronic link from which the changed qualified certificate can be downloaded.

When the Signature Owner/Author or a person authorized by him/her visits the Registration Authority, the user receives the new certificate on site. An authorized officer of the Registration Authority shall record the new qualified certificate on a signature/seal creation device, which also generates the cryptographic key pair for the certificate.

4.8.5 CONFIRMATION OF ACCEPTANCE OF A NEW QUALIFIED CERTIFICATE

Upon receipt of a changed qualified certificate, the user undertakes to verify its content especially regarding the accuracy of the data and the availability of a public key corresponding to the private key it owns. If the certificate has any errors that cannot be accepted by the user, the certificate must be terminated immediately.

If the issued certificate contains errors or omissions, the Signature Owner/Author or the person authorized by him/her may object within 3 (three) days of its publication in the register. Evrotrust shall remove them by issuing a new qualified certificate without payment of remuneration unless they are due to the provision of false data. In the absence of an objection, the content of the certificate shall be deemed to have been accepted.

4.8.6 PUBLICATION OF A NEW QUALIFIED CERTIFICATE

Evrotrust, through the Operational Certification Authority, shall immediately publish the changed qualified certificate in the certificates register.

4.8.7 INFORMATION FOR RELYING PARTIES

The public key in the qualified certificate corresponding to the private key held by the Signature Owner is publicly available to all relying parties.

Each relying party, including an operator at the Registration Authority, should use the public key and the certificate of the Signature Owner/Author in accordance with the requirements of the policy indicated in the certificate.

Relying parties must use the public key only after checking the status of the certificate and verification of the electronic signature of Evrotrust.

It is of particular importance that relying parties do not use the public key after termination of the certificate or at a time when it is suspended.

4.9 SUSPENSION AND REVOCATION OF A QUALIFIED CERTIFICATE

Suspension and revocation of the validity of a qualified certificate is an established operational practice of Evrotrust. They shall be only executed during the validity period of the certificate. Suspensions shall lead to temporary suspension of the certificate. Revocation shall lead to irrevocable termination of the certificate's validity and is an irreversible process.

If a certificate has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

If Evrotrust suspends or revokes the certificate's validity, it shall register this change in its certificate database and shall publish the revoked certificate status in a timely manner but in any event within 24 (twenty-four) hours of receipt of the request. Suspension or revocation shall take effect immediately after being published in the certificates register. They are always clearly marked with the exact date and time of the status change in the corresponding Certificate Revocation List (CRL) and in the Online Certificate Status Protocol (OCSP).

Upon revocation of the certificate of the Operational Certification Authority for issuance and maintenance of qualified electronic signature/seal certificates, the effect of any certificates issued by this Authority that are still valid shall be terminated.

Only the Operational Certification Authority that has issued the qualified electronic signature/seal certificate may suspend the effect of this certificate.

If the revocation is a result of an operator's error or a result of a compromise of an operational private key of Evrotrust, which has led to the revocation of the certificate of the Operational Certification Authority, the Provider shall issue an equivalent qualified certificate at its own expense.

Suspension and revocation management services for a qualified certificate are available 24 hours a day, 7 days a week.

In cases of failure in the system, services or other factors that are beyond the control of the Certification Authority, Evrotrust shall do its utmost to ensure that the service is not absent for a period longer than the maximum period of time, which in this case is 3 (three) hours.

Evrotrust shall provide all relying parties with information on the validity or non-validity of the qualified certificates issued by it. This information shall be available at any time even after the expiry of the validity period of the certificate in an automated and reliable way.

The time in the systems associated with the suspension and revocation of certificates shall be synchronized to UTC at least once every 24 hours.

4.9.1 REASONS FOR REVOCATION OF A QUALIFIED CERTIFICATE

The main reason for revocation of a qualified certificate of a user is the loss of control over the private key or the medium on which it has been recorded, or even a suspicion of such loss. Circumstances exist when the private key owned by the user is outside its scope of security, when there is a material breach of the Signature Owner/Author's obligations described in the contract between him/her and Evrotrust, or the requirements of the Practice and Policy for the provision of Qualified Certification Services are not met.

Evrotrust shall revoke a qualified certificate issued by it in the following circumstances:

- when the information entered in the certificate has changed;
- when there is a suspicion that the private key associated with the public key contained in the certificate is compromised - unauthorized access to the private key has occurred, or there is a reason to suspect such access, loss of a private key or having reason to know about such loss, theft of a private key or having reason to know about such theft, accidental deletion of a private

key;

- the user decides to terminate the contract with Evrotrust;
- death or placing under full interdiction of the Signature Owner/Author by termination of the legal entity of the Author;
- termination of the representative authority of the Signature Owner to the Author;
- when the user does not meet the requirements of the adopted authentication policy;
- if the Certification Authority has ceased its activity;
- if the user owes outstanding fees for the provision of qualified certification services;
- when reliability and security of the private key of the Certification Authority has been violated;
- when a user who has been an employee of an organization terminates his/her contract of employment and does not return the used cryptographic card on which the certificate and the corresponding private key has been stored;
- other circumstances related to non-compliance with the requirements of the Practice for the Provision of Qualified Certification Services.

Certificate that belongs to the Certification Authority may be terminated by its issuing authority. Such revocation may occur in the following situation:

- when the Certification Authority has reason to believe that the information in the issued certificate is incorrect;
- when the private key of the Certification Authority or its information system is violated in a manner affecting the credibility of the certificates issued by that authority;
- when the Certification Authority has materially breached an obligation arising from this Practice for the Provision of Qualified Certification Services.

Where certificates have been issued with a view to PSD2 compliance, termination requests in case of a change in the person's registration, shall be submitted with and are the responsibility of an NCA. Evrotrust verifies the authenticity of such requests. Additionally, Evrotrust requires that the NCA uses the following email address: support@evrotrust.com to send any requests related to a change in validity periods or termination of these certificates. Regardless of the message format chosen by the NCA, Evrotrust always verifies them.

4.9.2 GROUNDS FOR TERMINATION OF A CERTIFICATE OF A CERTIFYING AUTHORITY

A certificate which belongs to the certifying authority may be terminated by its issuing authority. Such termination may occur in the following situation:

- ❖ When the certifying authority has reason to believe that the information in the issued certificate is false;
- ❖ When the private key of the certification authority or its information system is violated in a manner affecting the credibility of the certificates issued by that authority;
- ❖ When the certifying authority has substantially breached an obligation arising from the present "Certification practice statement for qualified certification services".

4.9.3 PERSONS AUTHORISED TO REQUEST REVOCATION OF A QUALIFIED CERTIFICATE?

The following entities may request revocation of a qualified certificate:

- ➢ a user who is a Signature Owner/Author of a certificate;
- ➢ an authorized representative of the Certification Authority (in the case of Evrotrust, this role is reserved for the security administrator)
- ➢ an Author who as an employer terminates the employment contract of his or her employee and also terminates the certificate of the Signature Owner who is his/her subordinate. In this case, the employer shall immediately inform his/her subordinate;
- ➢ NCA;
- ➢ when an operator of the Registration Authority has doubts about the credibility of the information given by the user.

When a legal entity requests a certificate to be revoked by a person authorized by him/her (the Signature Owner), the Certification Authority must:

- ➢ verify that the applicant is authorized to request revocation;
- ➢ notify the Signature Owner.

A request for revocation of a qualified certificate may be submitted at the Registration Authority on paper, by telephone and online. When the user submits the request for revocation on paper, he/she must appear at the Registration Authority. In cases when an online revocation is requested, the request is required to be signed with a valid electronic signature/seal for the time being. In each case, the certificate is suspended temporarily for a grace period. Subsequently, an appearance at the Registration Authority is required for clarification of the case and confirmation of the request for revocation of the Qualified Certificate.

A Signature Owner may initiate revocation of a certificate from the Evrotrust mobile application by activating the relevant functionality when the certificate has been issued remotely. In this case, the Signature Owner is deemed to be identified, given the activation of the PIN for access to the application or through another biometric identifier.

4.9.4 PROCEDURE FOR REVOCATION OF A QUALIFIED CERTIFICATE

4.9.4.1 PROCEDURE FOR REVOCATION OF A QUALIFIED CERTIFICATE OF END USER

Revocation of the validity of a qualified certificate of end user shall be preceded by submission of a request for revocation before the Registration Authority of Evrotrust. The request for revocation of a certificate may be registered electronically only when the Signature Owner/Author has (another) valid and accessible for use qualified electronic signature/seal certificate. Otherwise, an on-site request shall be made before an authorized operator at the Registration Authority.

In case of a request for revocation, the Registration Authority shall register the request and start a procedure for its verification.

Evidence for revocation of a qualified certificate shall be submitted to the Registration Authority. After reviewing the evidence, the Registration Authority shall decide whether to proceed with the procedure for revocation or to reject the user's request for revocation of the certificate. The Registration Authority shall process and send an automated request to the Certification Authority to authorize the procedure for revocation.

Any request for revocation of a certificate must contain irrefutable evidence to confirm the revocation. All reasons for revocation must be validated (signed electronically or signed by hand).

The procedure for revocation of a qualified certificate shall be made as follows:

- The authorized operator at the Registration Authority, without identifying the user, shall immediately suspend the certificate's validity for a grace period.
- The Registration Authority strictly follows the requirements for identification and authentication of the Signature Owner/Author or the person authorized by him/her and the reasons for revocation. In all cases, the Signature Owner/Author or a person authorized by him/her must visit the Evrotrust Registration Authority for subsequent identification or to perform remote identification, respectively verification of the identity of the user.
- After a successful verification of the identity of the Signature Owner/Author or a person

authorized by him/her, the Registration Authority, through the authorized operator, shall submit a processed request to the Operational Certification Authority for revocation of the certificate. Upon confirmation by the Certification Authority, the request for revocation of the certificate shall be executed.

➢ Upon unsuccessful identification and verification of the conditions for revocation, the Registration Authority shall reject the request for revocation of the certificate and immediately notify the Signature Owner/Author or a person authorized by him/her of the reasons.

➢ A user with a rejected request for revocation of a qualified certificate may submit a new request for revocation of the certificate after removing the reasons given for the refusal.

Upon revocation of a certificate through the Evrotrust mobile application, the above procedures shall not apply. In this case, it is assumed that the request has been made by activating the relevant functionality in the application and the Signature Owner has been duly identified, given the knowledge of the PIN with which the application has been activated. Upon revocation of the certificate, Evrotrust through its Operational Certification Authority, shall immediately publish the revoked certificate in the CRL by issuing a new List and shall notify the Signature Owner/Author of the revoked certificate.

A revoked certificate shall not be subject to resumption or renewal.

Authorized personnel of Evrotrust shall have access to the revocation request and the system sampling documentation on the implementation of the revocation of a qualified certificate.

If a certificate is stored on an electronic cryptographic card, upon termination of the qualified certificate's validity, the card may be physically destroyed or securely deleted. This operation must be performed by the cardholder.

Evrotrust recommends the cardholder shall store it in a manner that prevents it from being stolen, unauthorizedly used or physically destroyed and the private key being deleted.

4.9.4.2 PROCEDURE FOR REVOCATION OF A QUALIFIED CERTIFICATE OF A CERTIFICATION AUTHORITY OR A REGISTRATION AUTHORITY

A certificate that belongs to a Certification Authority or a Registration Authority may be terminated by its issuing authority. In this case, authorized persons of the authority shall submit a request directly to Evrotrust.

Evrotrust may also submit a request for revocation of a certificate of a Certification

Authority or a Registration Authority.

4.9.5 GRACE PERIOD OF REVOCATION OF A QUALIFIED CERTIFICATE

Prior to terminating a valid qualified certificate, Evrotrust shall suspend its validity for a grace period. Within this grace period, Evrotrust shall process the request for revocation of the qualified certificate as it:

- shall carry out all checks to establish the identity of the applicant;
- shall identify the reasons for revocation of the certificate;

In case of unconfirmed reasons or after the expiry of the grace period, Evrotrust shall resume the validity of the certificate.

Evrotrust shall resume the validity of the certificate before the expiry of the grace period only at the explicit request of the Signature Owner/Author or a person authorized by him/her.

Suspension of a certificate shall not be allowed as a policy when the certificate has been issued remotely through the Evrotrust mobile application. In this case, the certificate shall be immediately revoked without a grace period and without the possibility of resumption.

Information on revoked certificates shall be stored in the Evrotrust database. Revoked certificates shall be published in the CRL within the required technological time, but for no longer than 3 hours.

Operators of the revoked certificates of the Certification Authority or the Registration Authority as well as the affected end-users shall be automatically informed of this revocation.

4.9.6 TIME LIMIT FOR PROCESSING THE REQUEST FOR REVOCATION

Request for revocation of a qualified certificate shall be processed by Evrotrust without undue delay.

4.9.7 CHECKING THE CERTIFICATE REVOCATION LIST (CRL)

Each relying party, upon receiving an electronic document signed with a qualified electronic signature/seal by the Signature Owner/Author shall be obliged to check the status of the qualified certificate in the current CRL or by checking the current status of the certificate in real time through the Validation Body of the certification authority.

The Certificate Revocation List, which each relying party may refer to, is located on the web site at: https://www.evrotrust.com.

Evrotrust shall not be responsible for damages and consequences of non-compliance with these requirements.

4.9.8 FREQUENCY OF ISSUING THE CERTIFICATE REVOCATION LIST (CRL)

Evrotrust through its Operational Certification Authority immediately publishes to the web address indicated in the certificate a new and updated CRL each time when a valid certificate issued by this Authority has been revoked.

The Provider, through its Operational Certification Authority, updates its Certificate revocation list (CRL) at least once on every 2 weeks if there is no suspension or revocation of a certificate during that period.

The validity period of at least 2 weeks is valid for each published new updated Certificate Revocation List (CRL) of the operational Certification Authority.

4.9.9 MAXIMUM DELAY OF PUBLICATION OF THE CERTIFICATE REVOCATION LIST (CRL)

Each Certificate revocation list (CRL) is published without any delay as soon as it is created, but not later than 60 minutes (1 hour) from including a new certificate in it.

4.9.10 ONLINE CERTIFICATE STATUS CHECKING

Evrotrust provides a qualified service for online status checking of issued certificates in real time. This service is based on an Online Certificate Status Protocol (OCSP) described in RFC 2560. Using OCSP allows to obtain information about the status of certificates without requiring verification in the CRL.

The OCSP work model is based on the "request-response" principle. Online access to the Validation Body shall be performed online. In response to each request, the OCSP server provides the following information about the status of a qualified certificate:

- ➢ good - which means a positive response to the request and must be interpreted as confirmation of a valid certificate;
- ➢ revoked - which means that the certificate has been revoked;
- ➢ unknown - which means that the certificate has not been issued by a Certification Authority of Evrotrust.

The OCSP service generates a database-based response. The OCSP response shall be valid for 7 days. In order to maintain proper performance of the system, OCSP responses shall be cached for a predetermined time usually for no more than a few hours.

4.9.11 REQUIREMENTS FOR ONLINE CERTIFICATE STATUS CHECKING

Certificate status checking in real time (under the OCSP) can be executed via the internet by using the OCSP protocol, which provides in an automated, reliable, free and efficient way information on the validity or revocation of issued certificates.

Relying parties should check this information they want to rely on. Evrotrust shall not be responsible for damages and consequences of non-compliance with these requirements.

4.9.12 SPECIFIC REQUIREMENTS REGARDING THE BREACH OF THE KEY SECURITY

In case of a breach of the security of the private key (its disclosure) by the Certification Authority or other entities operating within Evrotrust, the Provider shall immediately inform the relying parties.

4.9.13 REASONS FOR SUSPENSION OF A QUALIFIED CERTIFICATE

Evrotrust, through its Operational Certification Authority, shall suspend a valid certificate under certain conditions for a grace period.

The provider shall take immediate action on the request for suspension of a certificate.

For the period during which the certificate has been suspended, the certificate shall be deemed invalid and all electronic signatures/seals verified with this certificate shall be invalid.

Suspension and renewal of a certificate issued remotely through the Evrotrust mobile application shall not be allowed. Suspension of such certificates is excluded in this section and its subsections.

4.9.14 PERSONS AUTHORISED TO REQUEST SUSPENSION OF A QUALIFIED CERTIFICATE?

Evrotrust shall suspend the issuance of a valid certificate if:

➢ a request has been submitted by the Signature Owner/Author or a person authorized by him/her, without being obliged to establish his/her identity or representative authority;

➢ a request has been submitted by a person who appears to be aware of breach of the security of the private key;

➢ a request has been made by the Communications Regulation Commission (CRC);

4.9.15 PROCEDURE FOR SUSPENSION AND RESUMPTION OF A QUALIFIED CERTIFICATE

Suspension of the validity of a qualified certificate shall be preceded by submission of a request for suspension before the Registration Authority.

- The request for suspension of a certificate may be registered electronically or submitted on paper to an authorized operator at the Evrotrust Registration Authority.
- The request for suspension of a certificate submitted electronically shall be certified by an electronic signature/seal corresponding to the valid certificate of the Signature Owner/ Author.
- The authorized operator at the Registration Authority, without identifying the user, shall immediately suspend the certificate's validity. Suspension of the certificate shall be executed by its temporary entry in the CRL.
- After successful authentication of the authorized operator's identity at the Registration Authority before the Operational Certification Authority, the latter executes the confirmed request for suspension of the certificate.
- The registration authority cannot reject a request for suspension.
- After suspension of the certificate, the Provider, through its Operational Certification Authority, shall immediately publish the suspended certificate in the CRL by issuing a new List.
- After suspension of the certificate, the Provider shall immediately notify the Signature Owner/ Author of the suspended qualified certificate.

4.9.16 GRACE PERIOD OF SUSPENSION OF A QUALIFIED CERTIFICATE

Evrotrust shall suspend a qualified electronic signature/seal certificate for a grace period until the reasons for the suspension are specified.

4.9.17 RESUMING THE VALIDITY OF A SUSPENDED CERTIFICATE

Evrotrust shall resume a suspended certificate:

- in case the reasons for suspension have been removed before expiry of the period of suspension;
- at the request of the Signature Owner after clarifying the reasons for the requested suspension;

After resuming the validity of a certificate, the latter shall be deemed valid.

4.9.18 PROCEDURE FOR RESUMING THE VALIDITY OF A QUALIFIED CERTIFICATE

The Registration Authority shall resume a suspended certificate after receiving a request for resumption by the Signature Owner/Author and after a successful identification and verification of the identity.

The Registration Authority shall immediately resume a suspended certificate after the expiry of the grace period of suspension.

In all cases, the procedure for resuming a certificate shall result in removing the suspended certificate from the current CRL and a new CRL shall be published.

4.10 CHECKING THE CURRENT STATUS OF QUALIFIED CERTIFICATES

4.10.1 SPECIFICATIONS

Information about the status of the certificates issued by Evrotrust can be obtained from the CRL, which is published on the website of Evrotrust, through the OCSP.

The authentication services for the status verification of qualified certificates are available 24 hours a day (non-stop).

Evrotrust maintains the status of the already issued Qualified certificates during their validity period and after they expire.

4.10.2 ADDITIONAL FUNCTIONS

The service for online checking of the current status of the certificates by the OCSP shall be available for all types of qualified certificates and for all relying parties.

The internet address (URL) of the OCSP service is: http://ca.Evrotrust.com/ocsp .

The OCSP service is compulsory for all operational certification authorities and SSL certificates issued by Evrotrust.

For online verification of the status of certificates, Evrotrust applies the following requirements:

- The information on the status of termination is available after the period of validity of the certificates.
- Evrotrust does not remove the terminated certificates from the CRL after they have expired. The CRL includes the extension X.509 "ExpiredCertsOnCRL" as defined in ISO / IEC 9594-8 / Recommendation ITU-T X.509.
- In case Evrotrust decides to terminate the CRL, it issues and publishes the last CRL

with a value of the NextUpdate field, as defined in clause 6.3.9 of ETSI EN 319 411-1;

- Evrotrust maintains the integrity and availability of the latest CRL for at least 10 years;
- Evrotrust does not issue a final CRL until all certificates in the scope of the CRL have either expired or been terminated;
- When providing the OCSP service, the OCSP response will develop the ArchiveCutOff extension, as specified in IETF RFC 6960, with the archiveCutOff date set in the CA certificate "notBefore" date value. The extension will be returned in the OCSP responses only for expired certificates.
- When the CA certificate is about to expire, Evrotrust may calculate the last OCSP response for each issued certificate (whether terminated or not) by setting the value "99991231235959Z" via "nextUpdate".
- Evrotrust documents exactly in the current practice and General Terms and Conditions how the following requirements are met: a) the period during which the information on the state of termination is provided (item 4.9); (b) how the information on the termination status is provided to a certifying authority in the event of compromise (point 4.9); (c) how information is provided on the state of suspension in the event of the closure of Evrotrust (point 5.9).

4.11 TERMINATION OF A QUALIFIED CERTIFICATION SERVICES CONTRACT BY A USER

The qualified certification services contract between Evrotrust and a user shall be terminated:

- after the expiry of the validity of the last issued qualified certificate in case the user has not undertaken any action to update his/her certificate;
- when the qualified certificate has been terminated and the user has not taken any action to issue another certificate.

4.12 CONFIDENTIAL STORAGE OF A PRIVATE KEY (ESCROW)

The private keys of the Certification Authority of Evrotrust or of users, who are included in the certification hierarchy of Evrotrust, as well as the keys are personalized on removable media and are not subject to fiduciary storage by Evrotrust (ESCROW).

The private keys of users who have requested issuance of certificates remotely through the Evrotrust mobile application are stored encrypted using a reliable cryptographic system

(Hardware Security Module/HSM), certified for security level required by Regulation (EU) № 910/2014 г.

5. CONTROL OVER THE PHYSICAL AND ORGANIZATIONAL SECURITY

This part of "Practice in the provision of qualified certification services" describes the general requirements regarding the control of physical and organizational security, as well as the staff operations used in Evrotrust. It makes a review of the security requirements and procedures at the time of key generation, in the identification and verification of customers' identity, at issuing qualified certificates and their management, in Evrotrust auditing and archiving.

5.1 PHYSICAL SECURITY CONTROL

The measures taken with regard to the physical protection of Evrotrust are part of the Information Security system developed and implemented in Evrotrust, corresponding to the requirements of ISO/IEC 27001, ISO 9001, ISO 22301 and ISO/IEC 20000-1 standards.

The measures relating to the physical protection of information data, technology systems, premises and the related support systems are designed to prevent:

- ➢ Evrotrust controls the physical access to the facilities, the security of which is essential for the provision of trust services, and minimises any risks related to the physical security. The security of the systems for issuing and management of certificates is in line with the requirements of international standards and recommendations;
- ➢ the physical access to components of Evrotrust's system, the security of which is essential for the provision of trust services, is limited to authorised persons only. The criticality of the components is identified by risk assessment. Physical integrity is ensured with respect to the equipment located in the protected and isolated premises of Evrotrust. A two-factor control on the access and 24/7 armed physical security guarding has been implemented. No physical access to critical equipment is allowed for more than 30 (thirty) minutes per visit. The equipment cabinet may not be accessed by more than 2 (two) authorised technical staff members of Evrotrust. Any access to the premises with critical infrastructure is documented in special journals;
- ➢ control is applied for the purpose of preventing losses, damages or compromising of assets and interruption of the business operations. The authorised persons from Evrotrust's staff strictly observe the internal procedures for access to the different zones with restricted physical access;

- control is applied for the purpose of preventing compromising of data or theft of information processing tools. The physical protection of the premises where Evrotrust is located is ensured by their massive and stable construction with strong doors and keylocks. Protection is ensured by 24-hour non-armed security guarding. There is an Alarm System, a Video Surveillance System, a Signalling Alert System and an Access Control System in the premises of Evrotrust;
- the components that are critical for the secure operation of the trust services are located in a protected area, with physical security guarding against trespassing, with access control and trespassing detection systems;
- Evrotrust configures its systems by removing or deactivating all accounts, applications, services, protocols and ports that are not used in its activities.
- Evrotrust provides access to protected areas and high security areas only to trusted roles.
- The Root CA system of Evrotrust is in a zone with a high degree of security. The basic certification body of Evrotrust is located in a certified data centre.

Evrotrust provides physical protection and access control to premises where there are critical components installed in the infrastructure:

- Qualified Root Certification Authority – "Evrotrust RSA Root CA";
- Qualified Operational Certification Authority – "Evrotrust RSA Operational CA";
- Qualified Operational Certification Authority – "Evrotrust Services CA";
- Qualified Certification Authority for verification of status of Certificates issued by the basic Authority (OCSP service) "Evrotrust RSA Validation";
- Qualified Certification Authority for verification of status of Certificates issued by the operating certifying authority (OCSP service) "Evrotrust RSA QS Validation";
- Qualified Certification Authority for verification of status of Certificates issued by the operating certifying authority (OCSP service) "Evrotrust Services Validation";
- Qualified Time Certification Authority – "Evrotrust TSA";
- Registers and provider's web site;
- Registration Authorities.

The provider's infrastructure is physically and logically separated and is not used for other activities implemented by "Evrotrust Technologies" AD.

5.1.1 PREMISES AND STRUCTURE OF THE PREMISES

Evrotrust has a specially designed and equipped room with the highest degree of physical access control, which houses the provider's Certification Authority and all central infrastructural components.

5.1.2 PHYSICAL ACCESS

The physical security of the certificates issuance and management systems complies with the requirements of international standards and recommendations.

Physical integrity has been secured for the equipment in the protected and isolated area of Evrotrust. A two-factor access control and round the clock armed guards have been provided. Physical access to the critical equipment is not allowed for more than thirty (30) minutes per visit. Access to the equipment cabinet is not allowed for more than two (2) Evrotrust authorized technical persons. Each access to the critical infrastructure premises is documented in special journals.

The physical protection of the premises housing the Evrotrust equipment and the Registration Authority are built of massive and solid construction, with strong doors and locks. The protection is realized by a 24-hour unarmed security. The Evrotrust premises are equipped with an Alarm system, CCTV system, Intruder alarm system and Access control system.

All systems are periodically inspected.

The Evrotrust staff authorized persons strictly abide to the developed internal procedures for the access to different areas with limited physical access.

The access to the area of operators and administrators is limited and is administered using a smart-card system and access control.

Within the Evrotrust offices, the Registration authorities are differentiated and separated from the other rooms. They are fitted with equipment allowing the safe storage of data and documents. The access to these areas is monitored and restricted to authorized persons related to the registration authority's activity (registration authority operators, system administrators) and their customers.

5.1.3 ACCESS CONTROL

Evrotrust has an Access Control Policy in place, which is in line with the following requirements:

- access to the system is restricted to authorised persons only. Evrotrust ensures control on the access to sensitive information. The access rights for specific sites are defined by the privileges and roles of the employees;
- Evrotrust are administer user access of operators, administrators and system auditors applying the principle of "least privileges" when configuring access privileges. This generally applies to personnel appointed to trusted roles;
- the system administrator manages the user accounts and ensures timely modification or removal of access;
- access to the information and the applications is restricted in accordance with the Access Control Policy;
- Evrotrust's technological system ensures sufficient control on the computer security with respect to the administration and activities of the employees in accordance with their roles;
- Evrotrust controls the software use and the employees need to prove their identity before using critical applications related to the service;
- the employees of Evrotrust are responsible for their actions which is certified by journals of the events;
- Evrotrust ensures control on the access to sensitive information. The sensitive data are protected from disclosure by unauthorised users;
- TW4S provides an opportunity for control and restriction of access for identified persons to the system and user sites they own or they are responsible for. Evrotrust requires each user to prove their identity and to be successfully authenticated before allowing any actions on behalf of the respective user or role undertaken by the user. Second authentication is mandatory after logging off from the system. There are implemented mechanisms for privileged users, which reduce the risk during a certified user session and if the input device of the user is left unattended, the user session is terminated after a certain idle period. When the number of unsuccessful attempts for authentication by one and the same user reaches the maximum possible number of attempts, Evrotrust prevents any further attempts for authentication of the user until the administrator undertakes actions for unblocking the user (or within a certain period of time).

5.1.4 ELECTRICAL POWER SUPPLY AND AIR-CONDITIONING

The server cabinet with critical equipment is powered by two independent UPS systems and is shielded against external interventions. The air-conditioning in the isolated room maintains a constant air temperature for the normal operation of the technological system.

An external power supply by a diesel engine is maintained and reserved. In the event of a failure in the main power supply, the system switches to an emergency power supply (UPS and/or electricity). The operation environment in the computer systems area is monitored continuously and independently of the other operation areas.

The ventilation system has been specifically designed for this premises class, preventing the compromise to the physical and electromagnetic protection of this room, and to the normal operation of the installed computer components.

The internal Registration Authority of Evrotrust is connected to the emergency power system of the building.

5.1.5 FLOODING

To monitor the humidity in the computer systems rooms and in the whole Evrotrust building sensors have been installed to report the humidity level. These sensors are integrated into the Evrotrust building's security system. The guards and employees of Evrotrust are instructed and required in case of possible hazards to immediately inform the relevant services, the security administrator and the system administrator.

5.1.6 FIRE PREVENTION AND FIRE PROTECTION

Evrotrust complies with all standards for fire safety by conducting its business in accordance with all regulatory and standardization requirements in this area.

The protective room with critical infrastructure is located in a building in which have been installed: a sound and light fire alarm system, active fire alarm system with gas and gas stop button in complicated circumstances and evacuation. In case of fire, it is provided that the supply of electricity to the devices is switched off and the fire is extinguished by gas.

5.1.7 OPERATION WITH MEDIA

All media are securely processed in accordance with the requirements of the scheme for classification of information. The media that contain sensitive data that cease to be necessary are disposed of in a safe manner. All media containing software, data backups or auditing information are stored in a fireproof case in a special premise for backups with implemented access control. A system for physical and logical protection has been developed for the premise where the backup copies of Evrotrust are located. Evrotrust has undertaken serious measures against accidental or intentional damage to the data media. The registration authorities are obliged to keep and store the up-to-date information, including the users' documents on paper in a safe deposit box.

5.1.8 WASTE DISPOSAL

The provider has created a procedure for information destruction and waste disposal.

Paper and electronic media containing any relevant information about the Evrotrust security, after the expiry of the period determined in accordance with the internal rules of storage, are destroyed in special shredding devices.

The carriers of information about cryptographic keys and PIN/PUK numbers used for their storage are crumbled with appropriate devices. This applies to the carriers that do not allow a final deletion of stored data and its reuse.

In certain cases, the information from movable media is destroyed by deleting or formatting the device without the possibility of recovery.

5.1.9 LIFETIME OF TECHNICAL COMPONENTS

The lifetime of physical elements in the composition of all critical infrastructure components of Evrotrust is observed according to the operational requirements prescribed by the manufacturer, and after the intended period of operation, they are decommissioned.

5.2 ORGANIZATIONAL CONTROL

This part of the "Practice in the provision of qualified certification services" presents a list of trusted roles that can be identified by the Evrotrust staff. It also describes the responsibilities and obligations associated with any particular role. All procedures related to the security of the issuance, management and use of qualified electronic signature certificates/seals, are performed by the trusted Evrotrust staff. The provider maintains a sufficient number of qualified employees who, at any moment of its activities' performance, ensure compliance with applicable laws and the company's internal rules and regulations.

Evrotrust complies with the following requirements:

- Evrotrust guarantees that the employees and contractors observe the requirements for reliability of the operation;

- Evrotrust hires employees and, if applicable, subcontractors, that have the necessary expertise, reliability, experience and qualification and that have undergone a training on security and personal data protection rules relevant to the operations they perform;
- the employees of Evrotrust undergo periodical (at least every 12 months) training for increasing their expertise, experience and qualification. The trainings include courses in information security, potential threats and good security practices;
- proper disciplinary sanctions are imposed on employees who violate the policies of Evrotrust;
- the roles and responsibilities related to information security are documented in job descriptions;
- Evrotrust defines reliable roles which the security of the signatures/seals validation service is based on.
- the management of Evrotrust defines the responsibilities of the trusted roles;
- the trusted roles are approved and adopted by the management;
- Evrotrust's employees (both temporary and permanent) have job descriptions written with respect to the roles they perform, with division of the duties in accordance with the "least number of privileges" rule. The sensitivity of the position is defined based on the responsibilities, access levels, qualification and diploma;
- the job descriptions include requirements for skills and experience. A distinction is made in them between the general and specific duties;
- the employees apply administrative and operational procedures and processes that are part of the information security management procedures of Evrotrust;
- the management has the necessary knowledge with respect to the trust services provided, knowledge of the security procedures and experience in the field of information security and risk assessment sufficient for fulfilment of their management functions;
- all employees of Evrotrust with trusted roles are free of any conflicts of interest that could affect the objectiveness of the operations of Evrotrust;
- the trusted roles are described in section 5.2.1 of this document;
- the personnel of Evrotrust is assigned trusted roles by the senior management based on the "lowest privilege" principle with respect to access or during the configuration of the access privileges;

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

The following requirements are applied with respect to the management of Evrotrust's operations:

- Evrotrust, ensures the security and reliability of the trust services provided via regular internal and external audits performed by independent organisations;
- Evrotrust guarantees that the policy and practice applied in its operations is non-discriminatory;
- the trust services are available for all entities whose operations fall within the scope of applicability of the services and who agree to fulfil their obligations as specified in the policies, practices, the contract and the general terms of Evrotrust;
- in relation to the risk of liability for damages caused under Article 13 of Regulation (EU) No. 910/2014, Evrotrust concludes a suitable insurance policy for third party liability in accordance with the national law;
- Evrotrust has the necessary financial stability and resources for operation in accordance with this document;
- Evrotrust has policies and procedures for resolution of claims and disputes raised by users or relying parties in relation to the provision of the services or other activities related to the services;
- where the provision of trust services involves subcontractors, Evrotrust always signs a contract.

5.2.1 TRUSTED ROLES

A detailed allocation of the functions and responsibilities of the personnel is stipulated in the internal documents of Evrotrust: job descriptions, staffing plan and the relevant internal operating procedures.

The functions allocation is implemented in such a way as to minimize the risk of compromising, confidential information leakage or the emergence of a conflict of interests.

Evrotrust keeps qualified employees at positions ensuring the fulfilment of its obligations at any time during its activities of issuing, maintenance and management of qualified certificates in accordance with the regulations.

The provider ensures its activities with its own staff, while for certain activities under the

Regulation (EU) № 910/2014, Evrotrust may involve also foreign persons.

Evrotrust has developed job descriptions for each trusted role of the personnel, as follows:

- Security Administrator – overall responsibility for the management and implementation of systems security procedures: develops the security policy; takes measures for technical protection of data and systems; defines the operational security measures; exercises direct control over the compliance with the information systems' security requirements, monitoring the compliance with security procedures for installation, configuration, maintenance and changes in the information systems or the network.
- system administrator – responsible for the installation, configuration and maintenance of reliable systems for the services management: system recovery if necessary; reconfiguration of devices and systems in connection with the implementation of new services or solutions; monitoring of the technical and software status of the servers and alarms for incidents;
- System Operator – directly responsible for the operation of the reliable technological systems of Evrotrust and for the system backup: creation and management of certificates for qualified electronic signature/seal, including the creation of key pairs – private and public for a qualified electronic signature/seal; use of efficient technologies to ensure the daily operation of the system; testing and inspections for the reliable system operation and security; compliance with the technical requirements for the devices operation and in case of technical failure notifying the relevant officials;
- System Auditor – in charge of data storage, backup and management of event logs (especially for their integrity verification) in carrying out internal audits, as well as the compliance of the activity with Regulation (EU) № 910/2014. The system auditor supervises the activities of all registration authorities operating as assigned by Evrotrust.

5.2.2 REQUIREMENTS FOR THE DIVISION OF RESPONSIBILITIES

Evrotrust's employees (both temporary and permanent) have job descriptions written with respect to the roles they perform, with division of the duties in accordance with the "least number of privileges" rule. The sensitivity of the position is defined based on the responsibilities, access levels, qualification and diploma.

Evrotrust complies with the following requirements for division of duties and fields of responsibility:

- the roles and responsibilities, as described in the information security policy of

Evrotrust, are indicated in the employees' job descriptions;

- the trusted roles which Evrotrust's security of operations is based on, are clearly established;
- Personnel of Evrotrust are formally appointed to trusted roles by senior management responsible for security;
- Trusted roles shall be accepted by the appointed person to fulfil the role;
- the trusted roles are fulfilled by different employees;
- Evrotrust ensures that all employees with trusted roles are free of any conflicts of interest that could undermine their impartiality;
- the trusted roles and responsibilities included are security officers, system administrators; system operators and system auditors.

Certain trust services may require application of additional specific roles.

5.2.3 IDENTIFICATION AND VERIFICATION OF THE PERSONALITY FOR EACH ROLE

The Evrotrust staff is subject to identification and verification of personality in the following situations:

- when they are included in a list of persons with a limited access to Evrotrust buildings;
- when they are included in a list of persons with physical access to the Evrotrust technological system and network resources;
- when they are authorized to perform a specific assigned role;
- creation and assignment of an account and a password in the Evrotrust information system;

Any authorization for the performance of a certain role requires:

- The role to be unique and directly related to a specific person;
- not to be shared with another person;
- it should be limited to the function resulting from the role and to be performed by a specific person. The role is performed by providing software, technological system and access to the Evrotrust operating system. The proper execution of the role requires direct control over the position.

The operations, performed by Evrotrust, requiring access to shared network resources are protected by the implemented mechanisms for strong authentication and encryption of transmitted data.

5.3 CONTROL OVER THE STAFF

The Evrotrust staff consists of a sufficient number of highly qualified employees. The persons performing trusted roles have the necessary professional training and experience, which ensures the compliance with security requirements and technical standards for security assessment. The professional knowledge in the field of information systems, cryptography and infrastructure of public keys enables the employees with trusted roles to perform their official duties in high quality.

The Evrotrust employees pass periodic courses for subsequent additional training to meet the modern requirements for the Evrotrust activity.

5.3.1 STAFF QUALIFICATIONS

Evrotrust makes sure that the person performing a trusted role of the Certification Authority or in the Registration Authority system meets at least the following requirements for the position:

- has graduated at least secondary education (as far as there are no additional requirements for the corresponding job);
- Has signed a civil or labour contract describing his/her role in the system and the corresponding responsibilities;
- Has undergone the necessary training related to the scope of duties and the tasks of his/her position;
- Has been trained in the field of personal data protection;
- Has signed an agreement containing a clause on the protection of sensitive (in terms of Evrotrust security) information and the user data confidentiality;
- Does not perform tasks that may lead to a conflict of interest with the Evrotrust activity.

5.3.2 STAFF TESTING PROCEDURES

Each new Evrotrust employee, performing a trusted role is tested by Evrotrust:

- to confirm previous employment;
- for verification of recommendations;
- to confirm the educational degree;
- to verify the certificate of conviction;

- to verify the identity document.

In cases where the requested information is not available (for example, due to an applicable law), Evrotrust uses other legal methods, allowing the collection of the necessary information.

Evrotrust may reject the application related to the implementation of the trusted role or take action against a person who is already employed and performs a trusted role if it is established that:

- It was misled by an applicant or employee with respect to the above required data;
- receives highly unfavourable or not very reliable recommendations from previous employers;
- obtains information about any criminal record of the applicant or its employee has been sentenced by an enforced and valid judgment of court.

In the presence of any of these hypotheses, the further steps are carried out in accordance with the Evrotrust safety procedures and applicable law.

5.3.3 EVROTRUST STAFF TRAINING REQUIREMENTS

The personnel performing the duties and tasks arising from his/her employment in Evrotrust or the employment in the Registration Authority (in case of an external Registration Authority), must go through the following trainings:

- "Practice in providing qualified certification services" by "Evrotrust Technologies" AD;
- "Policy for the provision of qualified certification services" by "Evrotrust Technologies" AD;
- regulations, procedures and documentation related to the occupied position;
- security technologies and procedures related to security used by the Certification Authority and the Registration Authority;
- system software of the Certification Authority and the Registration Authority;
- responsibilities arising from roles and tasks performed in the system;
- procedures performed upon system failure or suspension of the Certification Authority's activities.

5.3.4 TRAINING FREQUENCY AND REQUIREMENTS FOR EMPLOYEES' SKILLS UPGRADING

The above described trainings are carried out regularly. These courses are complemented upon a change in the national legislation, in the sector, or upon a change in the documentation and operations of Evrotrust.

5.3.5 CHANGE OF JOB

The "Practice in the provision of qualified certification services" of "Evrotrust Technologies" AD does not imply any requirements in this area.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

In case of detection or suspicion of unauthorized access, the system administrator, together with the security administrator (Evrotrust employees) or only the system administrator (employee of the Registration Authority, in the presence of an external Registration Authority) may terminate the access of the perpetrator to Evrotrust or to the system of the Registration Authority. The further disciplinary actions are consulted with the Evrotrust management.

5.3.7 CONTRACT WITH THE PERSONNEL

Persons or consultants (e.g. software developers or consultants) may conclude contracts for the performance of trusted roles in Evrotrust. In such cases, they meet the same requirements applicable to the persons employed in Evrotrust.

Under a signed contract, the persons or consultants are subject to the same verification procedure as the Evrotrust employees.

5.3.8 DOCUMENTATION MADE AVAILABLE TO THE STAFF

The Evrotrust management and of the Registration Authority's management (in the case of an external Registration Authority) must provide their employees with access to the following documents:

- certification policies;
- certification practices;
- templates of requests, applications and declarations;
- abstracts of documents, corresponding to the performed role, including all emergency

procedures;

- set of responsibilities and obligations relating to the role performed in the system.

5.4 EVENT RECORDS AND LOGS MAINTENANCE

For the efficient management and operation of Evrotrust, all events having a significant impact on the security and reliability of the technological system, the control over the staff and users, and the impact on the safety of the qualified certification services, are recorded.

Each party, in any way related to the certification services provision, records the information and manages it appropriately. The data records compile registers of events and are stored in a manner permitting access of authorized individuals to this information (e.g. to resolve disputes between parties or detecting attempts to Evrotrust security violation). The recorded events are copied and archived. Backups are stored in safes.

Evrotrust are log all events relating to the life-cycle of certificates as all events relating to certificates generation and dissemination.

Where applicable, the event logs are created automatically. If it cannot be created automatically, the record is stored on paper. The entries are subject to audit.

The Evrotrust audit team carries out regular checks on the implementation of existing mechanisms, controls and procedures under the "Practice in the provision of qualified certification services", Regulation (EU) № 910/2014 and the current national legislation. The audit team evaluates the effectiveness of existing security procedures.

5.4.1 RECORD TYPES

Evrotrust creates records of any activity within its infrastructure. The archival records can be encrypted and stored on media, in order to be prevented from alteration or counterfeiting.

Such records are divided into three separate categories:

- Records of the technological system – when new or additional software is installed; upon startup of systems and applications thereto; in successful attempts to launch and access to hardware and software PKI-components (Public Key Infrastructure of the systems); generation and management of the key pairs and certificates for the certifying authorities and the Evrotrust infrastructure components; crypto modules' management; content of certificates issued; generation and management of key pairs and User certificates; launch of the systems and applications therein; while trying to launch and access the hardware and software PKI-components of the systems; generating a list of cancelled and revoked licenses (CRL); publication of valid certificates in the certificates register; Configuration of profiles of certificates; real-time-stamp certificate status; authentication of the time of a delivered content;

- errors – the records contain information about errors at the level of network protocols; upon a failure of the systems and the applications thereof; upon unsuccessful attempts to start and access the hardware and software PKI-components of the systems; upon system software and hardware systems failures and other anomalies in the platforms;
- audits – the records contain information relating to the qualified certification services, for example: received registration documents – for the purpose of identity check and identity verification; requests for issuance, renewal, suspension/resumption and termination of certificates; internal procedures for the identification and registration; release of a List of cancelled and revoked licenses (CRL), etc.

The records include information related to:

- the type of event;
- event identifiers;
- date and time of the event;
- identifier or other data allowing determination of the person responsible for the event;
- whether the event is associated with a successful or wrong result.

Records are stored which were created by the communication components in the infrastructure.

Records of old and current versions of the "Practice in providing qualified certification services" are stored as well as of the "Policy for the provision of qualified certification services", templates of requests, queries, operating instructions, etc.

Only authorized persons from the Evrotrust staff have access to the information in the records.

5.4.2 COLLECTION OF EVIDENCE

Evrotrust has a procedure of evidence collection which includes:

- Evrotrust records and keeps accessible for an appropriate period of time, including after its activities have ceased, all relevant information concerning data issued and received during its activity, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service;

- Evrotrust has undertaken appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage of personal data;
- Evrotrust is a company registered in the Republic of Bulgaria, within Europe, and as such, while complying with the European and national legislation, it ensures that ensures that personal data are processed in accordance with Regulation (EU) 2016/679. In this respect, by providing trust services remotely, Evrotrust provides access to its services by processing only those identification data that are adequate, relevant and not excessive;
- maintains the confidentiality and integrity of current and archived records concerning operation of services;
- records concerning the operation of services are completely and confidentially archived in accordance with good business practices;
- records concerning the operation of services are made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings;
- the precise time of significant operation management events, such as key management and clock synchronisation, are recorded;
- the time used to record events as required in the audit log is synchronised with UTC at least once a day;
- records concerning services are held for a period of time as appropriate for providing necessary legal evidence and as notified in the General Terms and Conditions and the contract;
- the events are logged in a way that they cannot be easily deleted or destroyed, except if reliably transferred to long-term media, within the period of time that they are required to be held.

5.4.3 FREQUENCY OF RECORDS CREATING

The information on the electronic logs is automatically generated.

In order to detect possible illegal activities, the security administrator, the system administrators and the auditor analyse the information at least once within one working day.

The security administrator is obliged to review and assess the accuracy and completeness of registered events and to verify the compliance with the Evrotrust security procedures.

The records in the events register are reviewed in detail at least once a month. Each event is subject to explanation and is described in the event log. The process of the events log review includes a check for its forgery or alteration.

5.4.4 PERIOD OF RECORDS STORAGE

Registered events record logs are stored in files on the system drive for at least six (6) months. During this time they are available online or upon search by any authorized Evrotrust official. After this period, the records are stored in the archives.

Archived logs are stored for at least 10 years.

5.4.5 PROTECTION OF RECORDS

The archive is signed with a digital signature and an electronic time-stamp. The information from the entries in the logs is periodically recorded on physical media which are stored in a special safe located in a room with a high degree of physical protection and access control.

A protocol of event logs may be reviewed only by the security administrator, the system administrator or the auditor. The access to the event log is configured in such a way, that:

- only authorized persons are entitled to read the registry entries;
- only the security administrator can archive or delete files containing registered events (after their archiving);
- it is possible to detect any tampering;
- Evrotrust ensures that the records do not contain gaps or forged entries;
- persons not authorized to change the contents of the logs do not have access to them.

Evrotrust implements the procedures for registered events protection in such a way that even after the logs are archived, it is impossible to delete records before the period of the archive maintenance.

5.4.6 KEEPING BACKUP COPIES OF EVENTS RECORDS

Backup copies of entries in the system logs are kept and reliably stored. These copies are created by persons authorized by Evrotrust.

The Evrotrust security procedures require event logs to undergo backup in accordance with an approved schedule, but not less than four times a year.

5.4.7 NOTIFICATION SYSTEM AFTER RECORDS ANALYSIS

Evrotrust has developed a procedure for the analysis of event records, implemented in the system which allows examination of current events and automatically notifies of threats or security breach. In the case of activities having an impact on the system security, the security administrator and the system administrator are automatically notified. In the other cases, the notification is addressed only to the system administrator.

When critical information is being transferred to authorized persons, in terms of system security situations are foreseen where the transfer is carried out by other, suitably secured communication means such as mobile phones, e-mail.

The competent authorities have the obligation to take appropriate measures to prevent an established threat.

5.4.8 VULNERABILITY AND RISK ASSESSMENT

Evrotrust classifies and maintains registers of all assets in accordance with the requirements of ISO/IEC 27001. Under the Evrotrust "Security Policy" analysis is made for vulnerability assessment on all internal procedures, applications and information systems. Requirements for analysis may also be defined by an external institution, authorized to audit Evrotrust.

The risk analysis is carried out at least once a year. The decision to proceed with the analysis is made by the Board of Directors.

The security administrator controls the preservation of security logs records, the proper backup archiving, the activities implemented in case of threats and the compliance with the current Practice.

Evrotrust complies with the following requirements related to the risk assessment:

- Evrotrust performs risk assessment in order to identify, analyse and evaluate the risks associated with the provision of trust services by taking due account of the business and technical issues;
- Evrotrust selects appropriate risk treatment measures, by taking due account of the risk assessment results. The risk treatment measures ensure that the level of security is commensurate to the level of risk;

- Evrotrust determines all security requirements and operational procedures that are necessary for implementation of the selected measures for risk treatment, as documented in the Information Security Policy and in the Practice for provision of qualified trust services;
- the management of Evrotrust regularly reviews and revises the risk assessment; the management of Evrotrust shall approve the risk assessment and accept the residual risk identified.

5.5 ARCHIVING

The information on significant events is periodically electronically archived.

Evrotrust archives all data and files related to: the registration information; the system security; all requests submitted by users; the whole user information; all keys used by the Certification Authorities and the Registration Authority; and the whole correspondence between Evrotrust and the users. All documents and data used in the process of identity verification are subjected to archiving.

The provider keeps the records in a format allowing reproduction and recovery.

5.5.1 TYPES OF ARCHIVES

Evrotrust manages two types of archives: paper and electronic.

5.5.2 PERIOD OF ARCHIVES STORAGE

Archived data (paper and electronic) are stored for a minimum of 10 years. After this storage period, archived data may be destroyed.

5.5.3 PROTECTION OF ARCHIVAL INFORMATION

Evrotrust stores archived records in a way excluding unauthorized and untrusted individuals having access thereto. The information archived electronically is protected against unauthorized viewing, modification, deletion or falsification through the implementation of an Access control system (via accounts and passwords). For the purposes of archiving reliable electronic media are used that cannot be easily destroyed or deleted during the storage period.

For the purposes of the safe storage of archive files in electronic form, they contain an electronic signature.

The electronic communications between the local infrastructural components are protected on the basis of the PKIX standard.

Remote electronic communications are protected and are based on the PKIX standard.

The provider assesses the use of postal and courier services and fax with the Users.

5.5.4 RECOVERY OF ARCHIVED INFORMATION

The possibility the backups to be fully restored (e.g. after a system failure) is essential for the proper functioning of Evrotrust.

Detailed procedures for archiving, creation of copies and system recovery after accidents are described in the technical documentation of Evrotrust, with "Internal" status. This documentation is available only to the authorized personnel and inspection bodies.

5.5.5 REQUIREMENTS FOR THE ARCHIVING TIME RECORDING

Archive records are secured by authentication of the exact time of their signing.

5.5.6 ARCHIVE STORAGE

The archive data collecting system is an Evrotrust internal system. Exceptions to this rule are the archives collected by the Registration Authority.

Archival information (on paper and electronic media) is properly stored in a special safe, in a room with a high degree of physical protection.

5.5.7 ARCHIVAL INFORMATION ACCESS AND VERIFICATION PROCEDURES

Access to the archive is only available to authorized Evrotrust employees after a successful authentication and confirmation of access rights.

The data are checked periodically and compared against the original data to verify the integrity of archived information. This activity is supervised by the security administrator by keeping records for each stage of the procedure. The verification results are recorded in the respective registers of events.

If damages or modifications to the original data are identified, the damages are removed as quickly as possible, in accordance with the internal procedures and rules of Evrotrust.

5.6 ASSET MANAGEMENT

Evrotrust manages its assets by applying the following requirements:

- Evrotrust has provided a proper level of protection of its assets, including its information assets.
- Evrotrust maintains an inventory list of all information assets and classifies them based on the risk assessment.

5.7 PROVIDER'S KEY CHANGE

The provider can change the key corresponding to an issued certificate only issuing a new certificate or renewing the current one.

The private key of a Certification Authority can be changed in case of:

- expiry of the validity of its accompanying certificate;
- introduction of new services by Evrotrust, entailing changes in the private key characteristics (for example, changes relating to the security and a requirement for new applicable cryptographic combinations).

In case of a change in the private key of the Evrotrust Certification Authority the following rules are observed:

- the Certification authority, with whose key user certificates are signed, and whose key will be modified, suspends the issuing of certificates sixty (60) days prior to the moment when the remaining period of validity of the private key equals with the validity period of the last issued certificate;
- the Certification authority, whose private key signs the List of cancelled and revoked licenses (CRL) and whose private key will be changed, continues to publish lists signed with old private key until the moment when the last published certificate validity expires.

5.8 COMPROMISED KEYS AND RECOVERY AFTER ACCIDENTS

This part of the "Practice in the provision of qualified certification services" describes the procedures performed by Evrotrust in case of accidents (including natural disasters) to restore the service to the users. These procedures are performed in accordance with the adopted "Plan for post-disaster recovery".

For the cases of accident or threat of an accident procedures have been developed to deal with these unusual situations and to restore the normal operation of Evrotrust. Upon a possible threat of occurrence of accidents, analysis is made of the availability of critical resources needed to restore the system. Current recovery cost estimates are made as well. There are procedures for accidents with the IT and accidents in the business processes. For example, in the field of information technology, there are requirements for storage of system hardware resources, requirements for system data storage and for storage of specific (custom) hardware resources, location of system (work) stations, internet, intranet, etc.

This plan is tested annually and is subject to training by Evrotrust employees.

The Evrotrust plan for post-disaster recovery is designed to ensure full recovery of all the functions of Evrotrust within one week after a crisis affecting the major structures. Evrotrust tests its equipment in its structure to maintain the functions of the Certification Authority and the Registration Authority after a major crisis that would stop the functioning of the entire structure. The results of these checks are used for evaluation and planning activities. The goal is, if necessary, for example after a major crisis, Evrotrust's structure operation to be recovered as soon as possible.

5.8.1 ACTIONS IN CASE OF ACCIDENTS

Archival data containing information on requests for issuance, management and revocation of certificates, as well as the records of all issued certificates in the database are stored in a safe and reliable place and are available to Evrotrust upon a request by authorized persons in case of an accident.

For emergency actions, Evrotrust has developed a "Contingency plan", which is checked once a year.

Evrotrust must be able to detect any possible incident. After analysing of what happened, the aim is to prevent future incidents based on system errors or failures of services and technologies. To do all this, Evrotrust monitors all systems and services without interruption (24/7), and also has a telephone for information and assistance, where users can notify for incidents or faulty services.

The plan identifies the approximate time for detection of any kind of incidents. Evrotrust ensures that any potential incident can be detected. The provider is able to distinguish between real incidents and false alarms. Serious incidents are reported to the management. The plan identifies the approximate time for notification and confirmation. It defines the roles and responsibilities. It assesses the type of incident, the appropriate response time and the further actions. The events are recorded. The causes for the accident and way it has affected the work efficiency are documented. The measures taken (response time and recovery time of the service or system, etc.) are recorded. Improvements are proposed. This plan indicates what type of backup is performed, at what intervals, where to store the information and the structure, etc.

5.8.2 INCIDENTS, RELATED TO FAILURES IN HARDWARE, SOFTWARE AND/OR DATA

The whole information in case of theft of hardware, software and/or data is transmitted to the security administrator who acts in accordance with the internal procedures developed by Evrotrust.

These procedures are associated with analysis of the situation, investigation of the incident, measures to minimize the consequences and to prevent similar incidents in the future.

In the event of failures in the hardware, software or data, the Provider notifies the users, recovers the components of the infrastructure and resumes in priority the access to the provided trust services, to the web site and to the Certificate Revocation List (CRL).

For such cases, Evrotrust has developed an "Incident management plan". The provider has a plan to manage all incidents which affect the normal functioning of the public key infrastructure. This plan is in line with a Business plan, Business continuity plan and a Plan for post-disaster recovery.

5.8.3 COMPROMISED OR COMPROMISE-SUSPECTED PRIVATE KEY OF THE EVROTRUST CERTIFYING AUTHORITY

The provider takes the due care to maintain the continuity and integrity of the certification services related to the certificates issued, maintained and managed.

The provider takes its best care, within its capacities and resources, to minimize the risk of compromising the keys of its Certification authorities due to natural disasters or accidents.

In the event of a compromise or a suspected compromise of the private key of an Evrotrust Certification Authority, the following actions are taken:

- the operating authority's license is immediately terminated;
- the Certification Authority generates a new key pair and a new license;
- all license users are immediately informed about what happened, using the mass media (information on the Evrotrust page) and by e-mail;
- all trusting parties are informed;
- the certificate, corresponding to the compromised key is entered in the List of cancelled and revoked licenses (CRL), together with the appropriate reason for termination;

- all user licenses, issued by the certificate corresponding to the compromised private key are terminated and entered in the List of cancelled and revoked licenses, indicating an adequate reason for their termination;
- new certificates are issued to affected users;
- the new user certificates are issued at the expense of Evrotrust (users are not charged);
- an instant analysis is made and a report is prepared on the cause of compromising.

These operations are carried out according to the plan developed by Evrotrust for security incidents. This plan is developed by an Evrotrust team under the leadership of the security administrator and is approved by the Board of Directors of Evrotrust.

5.8.4 CONTINUITY OF BUSINESS AND RECOVERY AFTER ACCIDENTS

Evrotrust manages the continuity of its business by applying the following requirements in its operations:

- Evrotrust has developed an Operation Continuity Plan which is periodically tested and maintained up-to-date and which shall be adopted in case of an accident. This document governs the preparation and processes to ensure the preservation of the Evrotrust activity. The aim is to achieve continuity in the company's operations and business protection when there are major disruptions of normal commercial operations;
- In case of an accident and failure of critical components of the technological system, including hardware, software or compromising of a private key of Evrotrust, the operations are resumed within the delay period established in the continuity plan. The reasons for the accident are analysed, suitable measures for its elimination are undertaken and measures are defined to prevent its recurrence.

The security policy, followed by Evrotrust, takes into consideration the following threats influencing the continuity of the services provided:

- a failure in the Evrotrust computer system, including a failure of network resources – can occur by chance;
- a failure in software, malfunction or data access interruption – can occur through inappropriate applications or malware from users (such as viruses, worms, Trojan horses);
- loss of important network services relating to the interests of Evrotrust – can occur upon a collapse in the power-supply grid;
- compromising of a part of the network used by Evrotrust to provide its services.

To prevent or limit the losses of the above threats, as an adequate security policy, Evrotrust undertakes the following:

- all Signatories/Creators and trusting parties shall be informed as quickly as possible and in a way best suited to the existing situation;
- regular creation and archiving copies of all components of the Evrotrust infrastructure, stored in a well-protected and safe place;
- periodic creation of a backup copy of the database, including all filed requests, issued, renewed and revoked certificates. Backup copies are archived and stored in a well-protected and safe place;
- periodic creation of a backup copy of each server;
- Evrotrust private keys are divided in accordance with the security procedures and by secret sharing. They are kept by trusted individuals in a safe and protected place;
- the replacement of resources is done in a way allowing the recovery of the most recent data.

The post-accident system recovery procedures are tested on each component of the Evrotrust IT system at least once a year. These tests are part of the internal audit.

Software update is only possible after an intensive examination in a testing environment and actions in strict accordance with the described Evrotrust procedures. Any change in the system requires the consent and acceptance by the security administrator.

In every post-disaster system recovery the security administrator or the system administrator performs the following:

- If risk analysis identifies information requiring dual control for management, for example keys, then dual control is applied to recovery;
- changes all previously used passwords;
- removes all access rights to the system resources;
- changes all codes and PIN numbers associated with the physical access to the facilities and system components;
- if the recovery from the accident involves reinstallation of the operating system and utility software, all IP addresses in the system and its subnets are changed;
- Review analysis of the disasters causes.

5.9 TERMINATION OF EVROTRUST ACTIVITY

The obligations described below are designed to minimize disruptions to the users' and relying parties' activities arising from the decision of Evrotrust to cease operations.

5.9.1 OPERATION TERMINATION PLAN

Evrotrust has developed an Operation Termination Plan for ensuring continuity of service and specific scenarios thereto in accordance with the requirements of the *Regulation on the liability and for termination of the operation of trust service providers* and applies the following requirements:

- Evrotrust has adopted measures for minimising any potential interruptions of the trust services used by users and relying parties as a result of termination of the company operations. Particularly, Evrotrust ensures continuous maintenance of the information necessary for validation of the trust services correctness;
- Evrotrust has an updated Termination Plan;
- Before terminating its services Evrotrust informs all stakesignatorys, users, relying parties, providers, subcontractors or other parties it has agreements with and the respective supervisory bodies;
- Before terminating its services, Evrotrust terminates the authorisation of all subcontractors (if any) to act on their behalf in carrying out any functions related to the process of issuing trust service certification tokens;
- Before terminating its services, Evrotrust transfers its obligations to a reliable party for maintaining all the information necessary to provide evidence for its operation for a reasonable period, unless it can be proven that it does not hold any such information;
- Before terminating its services, Evrotrust destroys or withdraws its private keys, including backup copies (if any) from use in a way that prevents their retrieval;
- Before terminating its services, where possible, Evrotrust undertakes measures for transferring the trust services provided for its existing users to another qualified trust service provider;
- Evrotrust has an insurance for covering the costs, as far as possible, in case of bankruptcy or if it is otherwise unable to cover the costs, however, within the limits of the applicable legislation with respect to insolvency;
- Evrotrust maintains or transfers its obligations to make its public or certification

tokens available to relying parties for a reasonable period of time to a reliable party.

5.9.2 REQUIREMENTS RELATING TO THE TRANSITION TO THE CESSATION OF THE PROVIDER

Before the certification authority terminates its services, it is obliged to:

- inform the Supervisory authority of its intention to terminate its services, in the event of a claim for declaring the company bankrupt, declaring the company invalid or another request for termination or commencement of liquidation proceedings. The notification shall be made four (4) months prior to the agreed date of termination;
- notify (at least 4 months in advance) its users of the decision to terminate its services;
- change the status of its certificates;
- terminate all user certificates within the period stated for the termination of its activities;
- inform all its users on the services termination;
- make the reasonable commercial efforts to minimize the violation of users' interests;
- pay compensations to users. The compensations must be proportionate to the remaining period of the certificates' validity;
- perform the necessary actions to allow the Supervising authority to keep the List of cancelled and revoked licenses (CRL).

If a Registration Authority, as an external organization, has decided to terminate the representation of Evrotrust relating to provided certification services, it is obliged to:

- notify Evrotrust of its intention to terminate the activity. The notification shall be made within four (4) months before the agreed date of termination;
- transfer to Evrotrust the entire documentation related to customer services, including the archive and the audit data.

5.9.3 CERTIFICATION AUTHORITY TERMINATION

Before the certifying authority terminates its services, it is required to:

- 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 consumers, 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 body;
- 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 can not 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;
- 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.

5.9.4 TRANSFER OF ACTIVITIES TO ANOTHER PROVIDER OF QUALIFIED CERTIFICATION SERVICES

To ensure the continuity of providing qualified certification services to the users, Evrotrust can sign an agreement with another qualified provider of certification services. In such case, Evrotrust shall:

- inform the Supervisory authority of its intention, but not later than 4 months before the date of termination and transfer of activities;
- make all efforts and care to extend the issued user certificates;
- notify the Supervisory authority and the Users in writing that its activities are taken over by another registered provider, as well as of its name. The notification shall be published on the

website of Evrotrust;

- ➢ inform the Users about the maintenance terms of the certificates transferred to the receiving Provider;
- ➢ change the status of operational certificates and duly transmit to the receiving provider the whole documentation related to the activities, along with all archives and all issued certificates (valid, cancelled and suspended);
- ➢ perform the necessary actions to transfer the information maintenance obligations to the receiving Provider;
- ➢ transfer the management of the already issued end-user certificates to the receiving Provider;

The receiving provider shall assume the rights and obligations of Evrotrust with its discontinued operations, and continue to manage the active certificates until the expiry of their validity.

The archive of the terminated Evrotrust must be transferred to the Provider which received the activity.

5.9.5 WITHDRAWAL OF THE EVROTRUST QUALIFIED STATUS OR THE QUALIFIED STATUS OF A PARTICULAR SERVICE

Upon the revocation of the Qualified status of Evrotrust or of any certification service provided thereby, it performs the following:

- ➢ Informs its users about its changed status, or that of its services;
- ➢ changes the status of its certificates;
- ➢ terminates issuance of new qualified certificates but continues to support and maintain the already active certificates until they expire;
- ➢ makes reasonable commercial efforts to minimize the violation of users' interests.

6. MANAGEMENT AND CONTROL OF TECHNICAL SECURITY

This part of the "Practice in the provision of qualified certification services" describes the procedures for generation and management of cryptographic keys and the related technical requirements.

Evrotrust uses only reliable and secure hardware and software, which are part of the company computer system. The computer systems where all critical components of Evrotrust's infrastructure operate are equipped and configured with tools for local protection of access to the software and information data. Evrotrust applies procedures for information security management for the entire infrastructure of Evrotrust in line with the generally accepted and international practices and standards.

In order to ensure the reliable operation and security of the computer systems lifecycle, Evrotrust performs activities in accordance with the following requirements:

- During the development of new systems, Evrotrust performs analysis on the security requirements as early as during the design and specification stage and thus guarantees the integration of security in the IT systems;
- Evrotrust applies a security policy and a procedure for control on alterations during updates, modifications of emergency and operating software and changes in the configuration;
- The procedures include documenting the changes;
- Evrotrust protects the integrity of the systems and information from viruses, malware and unauthorised software;
- Evrotrust develops and applies procedures for all trusted and administrative roles that have impact on the provision of services.
- Evrotrust specifies and applies procedures for ensuring that:

a) any available software protective and functional updates (security patches) are applied within a reasonable period after becoming available;

b) the protective and functional updates are not applied if they are likely to introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them;

c) the justification for refusing to apply any protective or functional updates are documented.

6.1 KEY PAIRS GENERATION AND INSTALLATION

Cryptographic key pairs for the Evrotrust operational certificates are generated and installed according to the instructions and procedures in this document. The generation is performed by authorized persons at Evrotrust observing the requirements of at least dual control. To create a signature a protective mechanism is used, with a safety profile established in accordance with the technical specifications defining the security levels.

The provider uses its private keys only for the purposes of its activities, as follows:

- to sign the issued operating certificates of the Certification Authorities in its infrastructure;

- ➢ to sign the issued and published Lists of cancelled and revoked licenses (CRL);
- ➢ to sign all issued and published certificates of electronic signature/seal of the Users.

The cryptographic key pair (private and public) of the electronic signature/seal certificates issued in the Evrotrust infrastructure is generated as follows:

- ➢ by the Signatory/Creator, with hardware and software under its control, but approved by Evrotrust;
- ➢ by an operator of the Evrotrust Registration Authority, with hardware and software under the control of the Evrotrust infrastructure;
- ➢ by Evrotrust, when the certificates issuing is requested remotely, through the mobile app of Evrotrust.

For the generation of a key pair of a qualified electronic signature/seal certificate, a device for electronic signature creation/sealing is always used, with a protective profile according to Regulation (EU) № 910/2014.

Only electronic signatures/seals, created by the private key of a key pair generated in a device for the creation of qualified electronic signature/seal have the character of a qualified electronic signature/seal.

The Signatory/Creator undertakes to use licensed software to work with the device for electronic signature/seal creation.

6.1.1 GENERATION OF A KEY PAIR FOR A CERTIFICATION AUTHORITY

The provider generates pairs of cryptographic (RSA) keys to the basic and the operating Certification Authorities using a hardware cryptographic system (HSM/Hardware Security Module) with security level FIPS 140-2 Level 3 or higher, respectively CC EAL 4+ or higher.

Authorized Evrotrust personnel, under at least, dual control, performs the steps of the generation, installation and storage of the key pairs of basic and operational Certification Authorities, respectively "Evrotrust RSA Root CA", "Evrotrust RSA Operational CA" and и „Evrotrust Services CA", in accordance with a documented internal procedure agreed and approved by the management of Evrotrust.

The procedure is performed in the presence of a member of the Evrotrust Board of Directors.

Prior to the generation of a base key pair of Evrotrust, procedure is made to access the installed crypto module (HSM/Hardware Security Module), by generating separately and independently from each other symmetric keys, stored on tokens, protected by a Personal Identification Number (PIN) for access. Each of the operator tokens contains a part of the keys for access to the crypto module. The management of the Evrotrust private keys stored in the crypto module requires two of the four sets of three roles operator tokens and the corresponding access PIN-s.

The access codes for the private key are independently shared among the Evrotrust authorized personnel, so that the personal activation of the access to the corresponding private key shall be impossible.

The created private keys of the Certification Authorities are stored separately on individual devices for qualified electronic signature creation, each being under the control of more than one authorized person from the Evrotrust personnel. The separate storage of the private keys and the individual control of the access to the stored parts of the Certification Authority private keys in individual devices for qualified electronic signature/seal creation prevents these keys of being compromised and/or subject to unauthorized reproduction outside Evrotrust.

Certification Authority keys and certificates are generated during a key generation ceremony involving only persons authorized by Evrotrust.

The keys and certificates of the Certification Authority may be generated only during a key generation ceremony in which only persons authorized by Evrotrust participate. Evrotrust generates a new CA certificate and takes all necessary actions before the expiry of this certificate in order to have continuity of services. The new certificate is generated and distributed in accordance with this document. The procedure is carried out at an appropriate interval between the date of expiry of the certificate and the last signed certificate, so that all parties having a relationship with Evrotrust (entities, users, trustees, etc.) are aware of this key exchange and to implement the necessary operations to avoid inconveniences and malfunctions. This does not apply in case Evrotrust ceases its activity before the date of expiry of its operating certificate for signing. Evrotrust documents the procedure for generating a key pair of certification bodies.

The generation procedure includes at least the following:

a) roles participating in the ceremony (internal/external from the Evrotrust).

b) the functions to be performed by each role and in which phases;

c) responsibilities during and after the ceremony; and

d) requirements of evidence to be collected of the ceremony.

Evrotrust draws up a report proving that the ceremony was carried out in accordance with that procedure and that the integrity and confidentiality of the key pair has been ensured. This report must be signed:

- For root CA: from the trusted role responsible for the security of the key services management ceremony (eg security officer) and a trusted person independent of the management of Evrotrust (eg notary, auditor) as a witness that the report has been properly recorded the ceremony;
- For operational CAs: from the trusted role responsible for the security of the key management ceremony (eg security officer) as a witness that the report correctly records the key management ceremony.

6.1.2 GENERATION OF A KEY PAIR OF A SIGNATORY/CREATOR

The key pair of a Signatory/Creator of qualified electronic signature/seal certificates is generated only on a device (external) approved by Evrotrust for the creation of electronic signature/seal, checked for security level and for successful work through the interfaces of the Evrotrust infrastructure.

When the key pair is generated in Evrotrust, a device for electronic signature/seal creation is always used. The private key of the generated key pair cannot be output from the device.

The control over the private key is by an access code. The Signatory uses the access code to the device in order to access the private key for the creation of a qualified electronic signature/seal.

When the key pair is generated at a Signatory/Creator, the Provider recommends it to use an approved device, in the Evrotrust infrastructure for the creation of a qualified electronic signature/seal or an equivalent one meeting the requirements of Regulation (EU) № 910/2014 and compatible with the Evrotrust infrastructure.

In the cases where the generation of the key pair is performed at the Signatory or the Creator, the same shall bear the full responsibility for the protection of the private key in order to prevent its compromise, disclosure, modification, loss or unauthorized use. The Signatory/Creator shall be responsible for any omissions or actions of persons authorized by them, delegated to generate, keep or store their private keys.

6.1.2.1 REMOTE GENERATION OF A KEY PAIR

The Signatory/Creator uses a specialized software provided by Evrotrust to realize the process of the cryptographic key pair generation and management.

The generation, use and storage of the private key have a very high level of security, guaranteed by the carrier itself. It is reliably protected by a personal identification number (PIN), which is known only to the Signatory/Creator.

The Signatory/Creator generates an electronic request for a qualified certificate in PKCS#10 format and sends it to Evrotrust. According to the recommendations of RFC 2314 - PKCS#10, the ASN.1 electronic request format contains DN, a public key and other attributes, all of which are signed with the private key.

A key pair can be generated remotely, upon a request for a remote issuance of a qualified electronic signature/seal certificate. In this case, the keys are generated on a hardware crypto module and the private key is stored in a form encrypted by the user with his access PIN code.

6.1.3 DELIVERY OF THE PRIVATE KEY TO THE USER

When the key pair is generated at Evrotrust, the Signatory/Creator or a person authorized thereby receives the private key and the issued qualified certificate on a device for electronic signature/seal creation at the Registration Authority of the provider.

Upon an initial issuance of a certificate on a device for electronic signature/seal creation, before the generation of a pair of keys, the device is initialized and the following access codes are created: User ("User") and Administrative ("SO"). Codes are created also for personal access to the private key and for a blocked device unblocking.

The initial User and Administrative access and device unblocking codes are provided to the Signatory/Creator or to a person authorized thereby in a sealed, opaque paper envelope.

The Signatory/Creator is obliged to change its initial User code for access to the device through the software provided along with it. Evrotrust recommends the Signatory/Creator to periodically change its User code.

In the event of a certain number of unsuccessful attempts to enter the correct code for access to the private key of the Signatory/Creator, the access thereto is blocked. In such cases, the Signatory/Creator must use the supplied corresponding unblocking code.

The above procedures are not applied upon a remote issuance of a qualified certificate through the Evrotrust mobile application. In this case, the key pair is generated in an Evrotrust hardware crypto module, while the private key is encrypted by the PIN-code of the Signatory/Creator. Evrotrust does not store information about the PIN code. The latter is used by the user only in the mobile application and only for the time when used.

6.1.4 DELIVERY OF USER'S PUBLIC KEY TO THE PROVIDER

Made solely by a Signatory/Creator where a key pair is generated and who should deliver its public key to Evrotrust for the needs of the process of qualified certificates issuing.

The Signatory/Creator shall deliver, through the Evrotrust Registration Authority, the public key for the generated key pair, through an electronic request, whose format is PKCS # 10. The request contains a public key and is signed electronically with the corresponding private key. By checking the signature authenticity, Evrotrust can establish also the reliability of the transmitted public key.

The Signatory/Creator can provide the electronic request on a carrier personally at the Registration Authority, along with the other documents under the Evrotrust Policy or remotely.

The Evrotrust Registration Authority is required to check the possession of the private key by the Signatory/Creator and confirm the request for qualified certificate.

The above procedures are not applied upon a remote issuance of a qualified certificate through the Evrotrust mobile application.

6.1.5 DELIVERY OF PROVIDER'S PUBLIC KEY TO THE TRUSTING PARTIES

Evrotrust public keys are published in the certificates of the Evrotrust Certification Authority in format X.509 v.3.

The certificates are published in the certificates register.

Each trusting party establishes its confidence to Evrotrust by adopting and installing the Evrotrust operating certificates in the systems under its control.

6.1.6 LENGTH OF KEYS

The length of the base Evrotrust key "Evrotrust RSA Root CA" is 4096 bits, with an applicable combination of asymmetrical and hash algorithms: sha384-with-RSA.

The length of the key pair of the operating Certification Authority "Evrotrust RSA Operational CA" is 2048 bits, with an applicable combination of asymmetrical and hash algorithms: sha256-with-RSA.

The length of the key pair of the operating Certification Authority "Evrotrust Services CA" is 4096 bits, with an applicable combination of asymmetrical and hash algorithms: sha256-with-RSA.

The length of the key pair of the operating bodies "Evrotrust TSA", "Evrotrust RSA Validation" and "Evrotrust Services Validation" can be 2048 bits, with an applicable combination of asymmetrical and hash algorithms: sha256-with-RSA.

The applicable combinations for the respective profiles are:

Qualifies certificate profile	Keypair type and length	Asymmetrical and hash algorithms used
Evrotrust Qualified Natural Person Certificate for QES	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust Qualified Natural Person Attribute Certificate for QES	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust Qualified Legal Person Certificate for QESeal	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust SSL Domain Validated Certificate	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust SSL Organization Validated Certificate	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust SSL EV Certificate	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust SSL PSD2 Certificate	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust Qualified Natural Person Certificate for AES	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust Qualified Legal Person Certificate for AESeal	RSA 2048 RSA 3072	sha256-with-RSA
Evrotrust Qualified PSD2 Legal Person Certificate for AESeal	RSA 2048 RSA 3072	sha256-with-RSA

Regardless of where the key pair for the issuance of a certificate for electronic signature/seal was generated, the key must have a length of at least 1024 bits for RSA and DSA algorithms, and 160 bits for ECDSA algorithms.

6.1.7 CRYPTOGRAPHIC ALGORITHMS

All algorithms used comply 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. In case the algorithm is compromised or becomes inappropriate, all of the keys involved are pre-generated.

For each supported profile, Evrotrust monitors the strength of each cryptographic algorithm used for this account. In case that one of the algorithms or parameters used is considered to be less certain or the validity of the certificate is expiring, it is updated or a new account is created.

Should any of the algorithms, or associated parameters, used by Evrotrust or its subscribers become insufficient for its remaining intended usage then Evrotrust shall inform all subscribers and relying parties with whom has agreement or other form of established relations. In addition, the Evrotrust shall make this information available to other relying parties. In such cases, Evrotrust undertakes the termination of all affected certificates.

6.1.8 PARAMETERS OF THE PUBLIC KEY

The public key parameters are listed in the certificate which the Provider issues for this public key.

The Signatory/Creator of a key pair is responsible for checking the parameters' quality of the generated private key. He is obliged to check the ability of the keys to encrypt and decrypt, including electronic signature creation and its verification.

The medium used to generate and store keys on the main components in the Evrotrust infrastructure - "Evrotrust RSA Root CA", "Evrotrust RSA Operational CA", „Evrotrust Services CA", "Evrotrust TSA", "Evrotrust RSA QS Validation", „Evrotrust Services Validation" and others is a crypto module (HSM) with a certified security level FIPS 140-2 Level 3 and CC EAL 4+, which meets the applicable regulatory requirements.

The devices for qualified electronic signature/seal creation and the secured environment for the generation and storage of Signatory/Creator's keys are with security level CC EAL 4+ and FIPS 140-2 Level 3.

All devices outside the Evrotrust infrastructure, which the users can use to generate the key pairs and store the private key for electronic signature/seal must be certified for security level CC EAL 4+ and a higher equivalent one.

6.1.9 KEY USAGE

The parameters of the key pair usage, in particular that of the private key, are contained in the certificate, issued by Evrotrust through the attributes "Key Usage" and "Extended Key Usage", meeting the standard X.509 v3. The use of any attribute of the areas mentioned is consistent with RFC 5280.

6.2 PROTECTION OF PRIVATE KEYS AND CONTROL ON THE CRYPTOGRAPHIC MODULE

Any user, Certification Authority operator and Registration Authority operator creates and stores private keys using a reliable system for its safety. The Certification Authority generates a key pair by user's request and delivers them in protected mode, informing the user of the rules of his private key storage and protection. When the certificate is requested remotely, through the Evrotrust mobile application, the transfer of the private key to the Signatory/Creator is not done.

If the cryptographic device where the private key is generated and stored is not to be delivered personally to the user, and an intermediary is used instead (e.g. a courier company), the issued certificate shall be invalidated until a confirmation is received by the user. The access code to the delivered cryptographic device are sent to the user via an independent secure canal (e.g. the mobile application of Evrotrust).

The private keys of the Evrotrust Certification Authority and the keys of users who have requested remote issuance of qualified certificates are stored in secure cryptographic modules (Hardware Security Module/HSM), certified for security level according to the requirements of Regulation (EU) № 910/2014.

The installed cryptographic modules are with the highest level of security according to international standards.

The secure cryptographic device operates only in its configuration, as described in the relevant certification documentation. The CA private signature key is stored and used in a secure cryptographic device that complies with the requirements of Regulation (EU) № 910/2014. When outside the secure cryptographic device, the CA private key is protected in a manner that ensures the same level of protection as provided by the secure cryptographic device. The private CA signing key is archived, stored, and restored only by personnel in trusted roles, using at least double control in a physically secure environment. The number of staff authorized to back up, store and restore the CA private signature key is kept to a minimum and is in line with Evrotrust practice. Copies of private keys are subject to the same or higher level of security control as the keys currently in use. When private keys and all copies are stored in a specially protected cryptographic device, Evrotrust provides access control to ensure that the keys are not accessible outside that device. The secure cryptographic device is not tampered with during transmission. Evrotrust protects the cryptographic device from tampering while it is being stored. Evrotrust ensures that the secure cryptographic device functions properly. Private signing keys stored in a secure cryptographic device are destroyed when the device is no longer in use. This destruction does not necessarily affect all copies of the private key. Only the physical copy of the key stored in the secure cryptographic device is destroyed.

6.2.1 CRYPTOGRAPHIC MODULES STANDARDS

The main components in the Evrotrust infrastructure "Evrotrust RSA Root CA", "Evrotrust RSA Operational CA" and „Evrotrust Services CA" use a reliable cryptographic system (Hardware Security Module/HSM), certified for according to the requirements of Regulation (EU) № 910/2014, which meets the statutory requirements.

The device for qualified electronic signature creation, where the private key of the Signatory/ Creators generated and stored is with security level CC EAL 4 +/FIPS 140-1 Level 2 or higher.

All devices for qualified electronic signatures creation outside the Evrotrust infrastructure, which the User can use to generate key pairs and to store the private key must be certified for security level CC EAL 4 or a higher equivalent level, corresponding to the requirements of Regulation (EU) № 910/2014.

6.2.2 CONTROL OVER THE USAGE AND STORAGE OF PRIVATE KEYS

The private keys of the Evrotrust Certification Authority are stored and used only in the cryptosystem (HSM/Hardware Security Module) and are accessible via access codes divided into several parts – known to authorized persons from the Evrotrust Personnel. The basic Evrotrust certification authority is in "Offline" mode.

Along with the generation of the Certification Authority's key pair is performed also the procedure for the private key (or key pair) storing in accordance with the established internal procedure. For the management of the Evrotrust private keys stored in the crypto module, two of four sets with the three roles of operator tokens as well as the corresponding personal identification numbers (PIN) are needed for access.

Initial keys archive is made – after the creation of all keys, and subsequently – after the re-generation of some of them. The archiving of private keys stored in the cryptosystem (HSM) with a security level FIPS 140-2 Level 3 is performed on a device with the same security level. To archive the keys, two of the four persons having tokens to access the cryptosystem (HSM) are needed. Archiving is done in a secure environment. After the archive (Backup), it is put in a safe at a remote location, with the necessary security measures.

The private key of the Signatory/Creators used only in the device for electronic signature/seal creation device or on a device with an equivalent security level (as required by Regulation (EU) № 910/2014) and is accessible via a personal access code. Along with the generation of a key pair for the Signatory/Creator, storage of the private key is made on an electronic signature/seal creation device.

The Provider does not in any way store or archive the private key of a Signatory/ Creator for electronic signature/seal creation, unless the certificate of qualified electronic signature is requested remotely through the Evrotrust mobile application.

6.2.3 SAFE STORAGE OF A PRIVATE KEY (ESCROW)

The rules described above are applied.

6.2.4 PRIVATE KEYS STORAGE

The Certification Authority's private keys are stored in separated parts on separate tokens with safety profile CC EAL 4+ or higher, whereas the access to each device is controlled with an access code by the relevant authorized person from the Evrotrust personnel.

The separate storage of the Certification Authority's private keys on several tokens and the personal control over the access to these devices prevents the keys from being compromised or being subjected to unauthorized reproduction outside Evrotrust.

The reproduction of Evrotrust private keys on a reserve crypto module after a defect on the operational one is made only in the presence of at least two authorized persons, each of which controls the access to his device.

Evrotrust does not keep copies of the Registration Authority operators' private keys.

The provider does not create copies of users' private keys, except for the cases of remote issuance of qualified certificates through the Evrotrust mobile application. The private key of the

Signatory/Creators stored only on a device for qualified electronic signature/seal creation and cannot be visualized on other devices. Upon a default on a user's device for qualified electronic signature/seal creation the User must replace it and request the issuance of a new qualified certificate.

6.2.5 PRIVATE KEY BACKUP

The Certification Authority's private key, used for the creation of qualified electronic signatures/seals will be archived for at least 10 years after the expiry of its validity or after its termination. The same requirement applies also for the public key certificate corresponding to the private key after its expiration or after its termination.

The Evrotrust expired or terminated certificates shall be accessible electronically for 10 years.

Evrotrust does not create backup copies of the Registration Authority's private keys and of users' private keys, except upon a remote request for qualified certificate through the Evrotrust mobile application.

6.2.6 TRANSFER OF A PRIVATE KEY IN A CRYPTOGRAPHIC MODULE

Transfer of a private key in a cryptographic module is carried out in the following cases:

- for protection, in the event of a backup of private keys stored in the cryptographic module (for example, in the event of compromise or malfunction of the cryptographic module);
- when needed to transfer the private key from the operational crypto module to another one (in case of failure of the operating crypto module or upon the need of destruction).

The transfer of a private key in a crypto module is a critical operation. Such an operation requires appropriate measures and procedures to prevent the disclosure of the private key or its alteration and falsification during the operation execution.

The transfer of a private key in a cryptographic module requires a recovery of the key from the cards of two of the four authorized officials in the presence of a member of the Board of Directors.

6.2.7 STORAGE OF A PRIVATE KEY IN THE CRYPTOGRAPHIC MODULE

Depending on the cryptographic module used, the Evrotrust Certification Authority's private keys are always stored in encrypted form. Regardless of the private key storage form, it is not accessible to unauthorized persons outside the cryptographic module.

6.2.8 PRIVATE KEY ACTIVATION METHOD

Provider's private key is activated by a shared system access code, the individual parts of which are known by more than one authorized persons from Evrotrust. Only in the presence of these persons, after entering all parts of the access code, access is allowed to the slot in the cryptographic module (HSM) and the private key is activated.

The private key of the Signatory/Creatoris activated by entering the user code for access to where the key is safely stored or using another method of identification with the same or higher security level.

6.2.9 PRIVATE KEY DEACTIVATION METHOD

A private key of the Evrotrust Certification Authority, located in a cryptographic module (HSM) is deactivated by the suspension of the logical access to that key. The deactivation requires resetting of the cryptographic module's memory. This terminates the possibility for access and use of the private key. Any private key deactivation is recorded in a journal.

A private key of a Signatories/Creators deactivated by a suspension of the logical access to the device for qualified electronic signature/seal creation or by its physical destruction when it is external. Thus the possibility to access and use the private key is definitively terminated.

6.2.10 PRIVATE KEY DESTRUCTION METHOD

A private key of the Certification Authority in a cryptographic module (HSM) is destroyed by deleting the key or the respective slot. If necessary, also the recovery media stored in the archive are destroyed. Any destruction of a private key is recorded in a journal.

The private key of the qualified certificate of a Signatory/Creatoris destroyed by its deletion from the qualified electronic signature/seal creation device or the physical destruction of the device when it is external.

6.2.11 EVALUATION OF THE CRYPTOGRAPHIC MODULE

Evrotrust uses a reliable cryptographic system (Hardware Security Module/HSM), certified for security level FIPS 140-2 Level 3. It is also certified for Qualified Electronic Signature Creation Device (QSigCD) and Qualified Electronic Seal Creation Device (QSealCD) in accordance with

Regulation (EU) № 910/2014. The certification is based on Common Criteria (CC) EAL4+ AVA_VAN.5.

6.3 OTHER ASPECTS OF THE KEY PAIR MANAGEMENT

The requirements described in this part of the "Practice in providing qualified certification services" are applied to the procedures for public keys archiving and the procedures describing the validity terms of the user keys and the certifying authority keys.

Evrotrust ensures that it uses private signing keys appropriately.

Evrotrust does not use private keys after the end of their life cycle and for purposes other than their intended purpose. The keys are used only in physically secure rooms. The use of private keys is compatible with the hashing algorithm, signature algorithm, and key length used to generate certificates, in accordance with this document. All copies of private signing keys are destroyed at the end of their life cycle.

6.3.1 PUBLIC KEY ARCHIVING

The Certification Authority public keys are contained in the issued Evrotrust operating certificates and are stored in an internal register. The public keys are available to the trusting parties and users by publishing the certificates on the Evrotrust website.

The Certification Authority public keys are archived and kept for at least 10 years after the validity period expiry or of the relevant certificates' termination. The purpose of the public key archiving is to enable the verification of the electronic signature/seal after removing the certificate from the certificates register. This is extremely important in case of certificate status inspection.

The public keys of Signatories/Creators are contained in the certificates issued for them, published in the certificates register.

The public keys of Signatories/Creators are stored in the certificates register and are periodically archived.

Each public key archive or any logical and physical destruction of a public key is recorded in a journal.

6.3.2 PERIOD OF VALIDITY OF QUALIFIED CERTIFICATES AND USE OF KEYS

The period of use of public keys is determined by the value of the field in its certificate describing the validity of the public key. The certificates validity and their corresponding private keys may be shortened in case of certificates' termination.

Maximum periods of use of qualified certificates:

Evrotrust RSA Root CA	20 (twenty) years
Evrotrust RSA Validation	5 (five) years
Evrotrust RSA Operational CA	15 (fifteen) years
Evrotrust Services CA	10 (ten) years
Evrotrust TSA	5 (five) years
Evrotrust RSA QS Validation	5 (five) years
Evrotrust RSA QS Validation	5 (five) years
Evrotrust Qualified Validation Service	5 (five) years
Certificates for end users	Not more than 3 (three) years

When a signing key is used after its certificate's expiration, the signature is invalid.

Six months before the expiry of a Certification Authority's qualified certificate, the Provider shall issue a new qualified certificate and generate a new key pair. The certificate shall be made public in accordance with the procedures described in this document.

6.4 ACTIVATION DATA

When the user is personally present at the Registration Authority, the private key activation data is used mainly by an operator of the Registration Authority. Users use authentication and access control to their private key.

In cases where the Signatory/Creator generates a key pair for a qualified certificate, they themselves create and manage the activation data.

When Signatory/Creator requests remotely the issuance of a qualified certificate through the Evrotrust mobile application, it creates a PIN code, which encrypts the private key generated in the Evrotrust hardware crypto module. The latter does not store data on the PIN code. It is used by the user to decrypt and activate the private key upon remote signing, by the Evrotrust mobile application.

Installing and restoring CA key pairs in a secure cryptographic device requires simultaneous control by at least two trusted employees. Activating and deactivating a secure cryptographic device is done in a secure manner. When users use a custom secure cryptographic device, associated data (e.g. PIN code) is used to activate it. Activation data is securely prepared and distributed separately from the secure cryptographic device

6.4.1 GENERATION AND INSTALLATION OF ACTIVATION DATA

Activation data are used in the initial issuance of a certificate, on a signature/seal creation device, before a key pair generation. In this case, the device is initialized and access codes are created: User ("User") and Administrative ("SO"). These codes allow personal access to the private key in the device and, if necessary, to unblock it.

The codes for access and unblocking the device for qualified electronic signature/seal creation is provided to the Signatory/Creator or a person authorized thereby in a sealed, opaque paper envelope.

The Signatory is obliged to change the initial User access code through the software provided with the device.

The provider recommends the Signatory/Creator to periodically change its User access code to the device for the creation of the qualified electronic signature/seal.

The Signatory/Creator should use the Administrative access code to unblock a blocked device.

When the Evrotrust mobile application is used, the access code is generated by the Signatory/Creator. The code is not kept by Evrotrust and is available for operation by the user only while the mobile application is active. To restore the personal code, the Signatory/Creator creates secret word. The secret word is not kept by Evrotrust.

6.4.2 ACTIVATION DATA PROTECTION

The Signatory/Creator is obliged to store and keep from compromising the access codes to the qualified electronic signature/seal creation device.

Users should know that upon several unsuccessful attempts to access the device, it is blocked (locked). In such cases, the user must use the provided Administrative access code to unblock the device.

The provider recommends the device activation data never to be stored together with the device itself.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

Activation data must always be kept in a single copy.

The personal identification number (PIN) for the access must be periodically changed.

Activation data can be archived.

6.5 COMPUTER SYSTEMS SECURITY

Evrotrust uses only reliable and secure hardware.

The computer systems on which all critical components of the Evrotrust infrastructure operate, are equipped and configured by means of local protection of the access to the software and computer data.

Evrotrust uses information security management procedures for the entire Evrotrust infrastructure in accordance with standards generally accepted in international practice.

For higher reliability and security of the systems, the technical and cryptographic security of the processes performed by them, Evrotrust performs a number of tests and inspections of the equipment and technologies used. Tests and inspections of computer systems are made in accordance with a methodology for security assessment (regarding: processors status – consumption, load, use, storage status; core memory state, padding in-out; status of storage, number of running processes; load balancing). They are performed both periodically and upon any change affecting the infrastructure security. These tests include vulnerability and penetration tests. Vulnerability test are performed in period no longer then 3 months.

For the computer systems' security management, Evrotrust takes into account the requirements of ISO/IEC 27001.

Evrotrust has a Council of Information Security, which is the controlling authority on information security. The Council participates in the analysis of information risks and is convened to discuss any issues or incidents related to information security.

Local network components (e.g. routers) are stored in a physically and logically secure environment. The configurations of local network components (e.g. routers) are periodically checked for compliance with the requirements set by Evrotrust. Evrotrust applies multi-factor authentication to accounts involved in issuing certificates. The Certificate Dissemination Application (OCSP) requires access control when trying to add or delete certificates and change other related information. The Revoked Certificate Status (CRL) application requires access control when trying to change termination status information. Evrotrust provides continuous monitoring of the systems and signalling in case of detection, registration of violations, as well as timely response to any unauthorized attempts to access its resources.

6.5.1 DEGREE OF COMPUTER SECURITY

The degree of security of the systems used in the Evrotrust infrastructure meets the legal requirements for the implementation of the Evrotrust activities and is determined by the Evrotrust Security Policy document.

6.5.2 INCIDENT MANAGEMENT AND MONITORING

Evrotrust performs monitoring and incident management by applying the following requirements:

- ➢ Evrotrust has created and introduced strict procedures for monitoring of the technological system operation, the access to the information system, as well as the requests for trust services;
- ➢ the monitoring activities analyse and report the sensibility of each piece of information collected;
- ➢ cases of unavailable service or abnormal system operations that show a potential breach of security, including intrusion into Evrotrust's network, are detected and reported;
- ➢ authorised employees of Evrotrust monitor the following events:
  - ✓ starting and suspension of the registration operations;
  - ✓ availability and use of the necessary services via Evrotrust's network;
- ➢ in the cases of breaches of Evrotrust's security, there are procedures in place for timely, rapid and coordinated response in order to limit the breaches of security;
- ➢ the security incidents alerts are tracked and reported by employees with trusted roles in accordance with the company procedures;
- ➢ Evrotrust has established a procedure to notify the relevant supervisory authorities in line with the applicable regulatory rules about any breach of the information security or loss of integrity that has a significant impact on the trust service provided, within 24 hours after detection of the breach;
- ➢ where the information security breach or loss of integrity is likely to adversely affect any natural or legal person that was provided with a trust service, Evrotrust notifies the respective

natural or legal person without undue delay;

- Evrotrust monitors its technological system and regularly reviews the audit journals in order to identify evidence for any misconduct. The company has developed automated mechanisms for processing of the audit journals and for alerting the staff for possible critical events related to security;
- The system generates warnings in a timely manner that alert for unusual events that could influence the system capability for server signing in accordance with the security requirements (e.g. user operations outside the standard working hours; actions caused by a non-human intervention; user operations beyond the standard regulated operations);
- for each newly detected critical vulnerability a plan for its resolution is developed within 48 hours after its detection;
- for each hazard, based on its potential impact, Evrotrust:
  - ✓ develops a plan for minimising the damages;
  - ✓ documents the facts and reports to the management.
- The procedures for incident reporting to the management and the response from the decisions taken are used so that the measures undertaken could minimise any damages and so that future measures are undertaken to prevent such incidents.

6.5.3 INFORMATION SECURITY POLICY

The Information Security Policy focuses on the requirements related to the strategy for operations, the regulations, the legislations and contracts, as well as on the current and possible environment of any threat to information security. The security policy contains statements, objectives and principles that shall govern all actions in the assignment of general and specific responsibilities related to the management of security to certain roles and processes for overcoming any deviations, breaches and emergency situations. More particularly, the Information Security Policy includes procedures that describe the mechanisms for control on the information security: access control, classification of information, physical security and security of the surrounding environment, assets, information exchange, remote work, software used, cryptographic mechanisms for control, security of communications, personal data protection and relationships with providers.

Evrotrust has an Information Security Policy in place, that has been developed and approved by the management, which includes the following:

- The Information Security Policy defines the approach of Evrotrust to the management of its operations;
- Any changes to the Information Security Policy are communicated to third parties (users, relying parties, supervisory or other regulatory bodies, compliance assessment bodies), where applicable;
- Evrotrust's information security policy is documented, implemented and maintained up-to-date;
- All employees of Evrotrust have been familiarised with the Information Security Policy;
- Evrotrust is responsible for compliance with the procedures described in the Information Security Policy in the cases where it subcontracts part of its operations. If there are subcontractors, Evrotrust defines their liability and ensures that they are bound to strictly apply all information security controls required by Evrotrust;
- The Information Security Policy of Evrotrust and the inventory of information security assets are reviewed at planned intervals from time to time or in the case of significant changes, in order to ensure their continued suitability, adequacy and effectiveness;
- Any changes that will impact the level of security provided are approved by an information security management body. The configuration of the systems of Evrotrust is regularly checked for changes which violate the information security rules. The maximum interval between two validations is based on the internal procedures of Evrotrust;
- The Information Security Policy documents the security controls introduced for personal data protection. During the processing of personal data, Evrotrust complies with all personal data protection regulations applicable to its operations, including, but not limited to Regulation (EU) 2016/679. The Personal Data Protection Policy is an integral part of the Contract for use of the services. In case of any change to the Personal Data Protection Policy, changes are published on Evrotrust's website: www.evrotrust.com. Evrotrust undertakes all the necessary steps, including technical and organisational measures, based on the risk level of the personal data processing performed, in order to ensure the data security so that no accidental or unauthorised destruction, loss, alteration, unauthorised disclosure, access or other illegal or unwanted event can be allowed that could compromise the security of the personal data processed. Evrotrust collects information the amount of which is proportionate to its purpose and

use. Each user gives their consent to the processing of personal data. This consent is declared by signing the Contract for trust services. The personal data are only used in relation to the provision of the specific trust service.

6.6 IT SYSTEM'S LIFECYCLE SECURITY

6.6.1 CONTROLS ON THE IT SYSTEM DEVELOPMENT

The software applications used in the Evrotrust IT system have been developed and implemented by highly qualified specialists. Before the introduction of new applications, they pass through the test period. The tests are made on separate systems, independent of those in regular operation.

All hardware changes are monitored and recorded. Upon the purchase of a new technical equipment, it is supplied with the necessary operating procedures and instructions for use.

Evrotrust monitors capacity requirements and forecasts future capacity requirements to ensure adequate processing and storage capacity.

The technological security of the system is guaranteed as follows:

➢ technological equipment is delivered in a manner allowing its tracking. An assessment is made of the route from the first point to the place of its installation;

➢ supply and replacement of technological equipment is made only with original hardware. The change is carried out by trusted and trained personnel.

6.6.2 CONTROLS FOR THE IT SYSTEM SECURITY MANAGEMENT

The purpose of security management control is to supervise the functionality of the technological system and to ensure that it functions properly and in accordance with the supplied production configuration.

The current configuration of the Evrotrust technological system, as well as any amendments and updates to the system are recorded and performed under control. The controls allow continuous checks of the technological system integrity, timely updating, and troubleshooting.

6.6.3 CRYPTOGRAPHIC CONTROLS

Evrotrust has introduced proper security controls for management of the cryptographic keys and all cryptographic devices during their entire lifecycle. Hash algorithms and asymmetric algorithms that meet the requirements set out in ETSI TS 119 312 are used for the generation of a cryptographic pair of keys (private and public). The applicable combinations of asymmetric and hash algorithms by duration with respect to the qualified electronic signature is as described in ETSI TS 119 312. A key length that meets the requirements of ETSI TS 119 312 is used: the length of the pair of keys for qualified electronic signature/seal of a user can be 2048 bits or 3072 bits, with the applicable combination of asymmetric and hash algorithms: sha256-with-RSA. The key shall have a length of at least 1024 bits for RSA and DSA algorithms and 160 bits for ECDSA algorithms.

Evrotrust generates pairs of cryptographic (RSA) keys of the basic and the operational certification authority by using a hardware security system (HSM/Hardware Security Module) with level of security FIPS 140-2 Level 3 or higher, or, respectively CC EAL 4+ or higher. Evrotrust uses all its private keys solely for the purpose of its activities as follows:

- to sign the operational certificates issued to the certification authorities in its infrastructure;
- to sign the Certificate Revocation Lists (CRL) that have been issued and published;
- to sign all qualified certificates for electronic signature/seal of the users that have been issued and published.

In case of provision of a remote signing service with an electronic signature/seal and a requested issuance of certificate from Evrotrust's mobile application, the private key is generated and stored in an encrypted form in the hardware security module of Evrotrust, which meets the requirements of Regulation (EU) No. 910/2014 for a qualified signature creation device (QSCD). The key encryption takes place through a PIN code created by the user, which ensures that he is the sole person with access for activation of the key. The qualified electronic signature/seal creation devices guarantee that by using proper technical means and procedures, the following will be achieved as a minimum:

- the confidentiality of the data used for creation of an electronic signature/seal is reasonably guaranteed;
- the date for creation of an electronic signature/seal will be practically seen only once;
- the data for creation of an electronic signature/seal are sufficiently secured and may not be extracted and the electronic signature/seal is reliably protected against forgery by using the currently available technology;
- the data for creation of an electronic signature can be reliably protected by the legal

Signatory/Creator of the electronic signature/seal against use by third parties.

6.6.4 IT SYSTEM SECURITY LIFECYCLE ASSESSMENT

The "Practice in the provision of qualified certification services" does not imply any requirements in this area.

6.7 NETWORK SECURITY

Evrotrust's infrastructure uses modern technical tools for information exchange and protection in order to guarantee the network security of the systems against any external interventions or threats. Evrotrust protects its network and systems from attacks by applying the following requirements:

➢ Evrotrust divides its systems into networks or zones to a functional, a logical and a physical zone (including by location) based on the risk assessment and the link between the reliable systems and services. Detailed description of the network configuration and the means for protection are presented in the infrastructure technical documentation. This documentation has an "internal" status and is only accessible for authorised persons;

➢ Evrotrust applies one and the same security controls for all systems located within the same zone;

➢ Evrotrust limits the access and communication between the zones to those that are necessary for performing the relevant operations. Any attempts for unauthorised access to the system are documented via an Intrusion Prevention System (IPS);

➢ Evrotrust expressly bans or deactivates the unnecessary links and services;

➢ Evrotrust regularly reviews the established set of rules;

➢ Evrotrust maintains all systems that are essential for its operations in two protected zones. The servers and critical technological system of Evrotrust are connected to an internal LAN network. The remote access to the infrastructure (PKI) network of Evrotrust takes place via a designated VPN server that has been installed and configured, which accepts authentication through a special name and password issued solely for this purpose to authorised persons involved in the issuance of an electronic signature/seal and the administration of the infrastructure (Public Key Infrastructure/ PKI);

➢ Evrotrust has a separate special network for administration of the IT systems and the operational network;

- Evrotrust does not use systems that are used for administration of the security policy for other purposes;
- Evrotrust separates the systems servicing the trust services from the systems used for development and testing;
- Evrotrust shall establish communication between distinct trustworthy systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure. The remote access to the infrastructure (PKI) network of Evrotrust takes place via a designated VPN server that has been installed and configured, which accepts authentication through a special name and password issued solely for this purpose to authorised persons involved in the issuance of an electronic signature/seal and the administration of the infrastructure (PKI). The vulnerability scan requested are performed once per quarter.
- If an external service with High Availability requirements needs to use a trust service, the external network connectivity thereto will also take place based on the High Availability requirements, which guarantee accessibility of the trust service in case of a failure of one of its components;
- Evrotrust performs regular scanning of the vulnerability of the identified public and private IP addresses and records the evidence from this process. In order to ensure reliable reports, each vulnerability scan is performed by an authorised person with the necessary skills, qualifications and tools and in compliance with the code of conduct and the requirement for lack of conflict of interests;
- After each update, modification or upgrade of critical applications, Evrotrust performs systems intrusion tests;
- Evrotrust records the evidence that each intrusion test has been performed by an authorised person with the necessary skills and tools, who complies with the code of conduct and has no conflict of interests, in order to ensure a reliable report. The penetration test are performed at least once per year.

A detailed description of the Evrotrust network configuration and the Evrotrust protection means are presented in the technical documentation of the infrastructure. This documentation has an “internal” status and is accessible only to authorized persons.

7. PROFILES OF QUALIFIED CERTIFICATES, CRL AND OF OCSP

Evrotrust issues certificates with profiles that meet the requirements set out in ITU-T X.509 [6] or IETF RFC 5280.

Evrotrust issues certificates with relevant profiles as follows:

a) for the issuance of certificates to individuals (excluding website certificates) (with applicable policies: LCP, NCP and NCP +) in accordance with the requirements of ETSI EN 319 412-2;

b) for the issuance of certificates to legal entities (excluding certificates for websites) (with applicable policies: LCP, NCP and NCP +): in accordance with the requirements of ETSI EN 319 412-3;

c) for the issuance of certificates for websites or devices (with applicable policy: PTC): in accordance with the requirements of ETSI EN 319 412-4.

7.1 PROFILE OF BASE ROOT CERTIFICATION AUTHORITY "EVROTRUST RSA ROOT CA"

Version	V3	
Serial number	6C 6E C9 BF 48 51 72 A5 4B D4 0F 27 78 62 52 45	
Signature Algorithm	SHA384RSA	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	20 May 2016 15:39:19 UTC	
Validit to	20 May 2036 15:49:19 UTC	
Subject	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (4096 Bits)	
Subject Key Identifier	74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	
Key Usage (critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=None	

7.2 PROFILE OF VALIDATION AUTHORITY

Evrotrust issues a certificate of response of reasonable duration.

Where the service is offered as an application to third parties (SVAs) who rely on Evrotrust certificate status information services and are unable to deal with the non-critical extension and therefore face operational problems, Evrotrust further provides verification via CRL.

When both OCSPs and CRLs are provided, Evrotrust configures OCSP responses for unissued certificates in a way that excludes the possibility of unissued certificates appearing in the CRL, in which case, if the response is "canceled", the reason is identified. Evrotrust monitors requests for unissued certificates as part of security procedures to verify that this is an indication of an attack.

a) Online certification status (OCSP)

The Evrotrust validation Certification authorities "Evrotrust RSA Validation" of the basic certification authority "Evrotrust RSA Root CA", "Evrotrust RSA QS Validation" of the operational certification authority "Evrotrust RSA Operational CA" and и „Evrotrust Services Validation" of the operational certification authority „Evrotrust Services CA" work and provide the qualified service "online real-time check of certificate status" in accordance with the internationally approved recommendation IETF RFC 6960.

The OCSP user sends a request to check the status of a signature/seal to the OCSP server and receives a response – a certificate of status, signed by the Validation authority. The reply contains information on the status of the inspected electronic signature/seal certificate, the validity period of the reply and has a testimonial character. The OCSP server which issues confirmations about the state of the qualified certificates has a specially generated key pair, issued especially for that purpose.

b) Version

Evrotrust, through its Validation Certification authorities, issues status certificates for the issued qualified certificates in a format, specified in the international recommendation RFC 6960. The version is entered in the issued status certificates.

c) Format

Evrotrust issues status certificates whose format is consistent with the requirements in the international recommendation RFC 6960.

d) BASIC ATTRIBUTES OF THE STATUS CERTIFICATES

- Version – version of the status certificate;
- Response Type – type of response on the status;
- OCSP Response Status – response status;
- Responder Id - Identifier of the validation service;
- Produced At - date and time of the status certificate issuance;
- Responses – information, uniquely identifying the qualified certificate, for which the request was sent and for which the validation authority issues this status certificate;
- Cert Status – status of the qualified certificate for which the request was sent;
- This Update – time of an issued CRL, on the basis of which the status certificate was issued;
- Next Update – validity time of the CRL, on the basis of which the status certificate was issued;
- Response Extensions – additional extensions, included in the response;
- OCSP Nonce – contains the same information, submitted at the request in the Nonce field;
- Signature Algorithm - algorithm used for the electronic signing of the status certificate;
- Certificate – Contains the qualified certificate of the Evrotrust validation authority.

The contents of the status certificate of Evrotrust are:

OCSP Response Status	• **successful (0)** – Valid response to the request; • **malformedRequest (1)** – The request does not meet the requirements of OCSP syntax; • **internalError (2)** – Internal error. Please, try again later; • **tryLater (3)** – The service is temporarily unavailable. Please, try again later; • **sigRequired (5)** – The request should be signed; • **unauthorized (6)** – The client is not authorized for the request.
Response Type	Basic OCSP Response
Version	1 (0x0)
Responder Id	[Unique identifier of the service authority]
Produced At	[date and time on UTC of the response generation]
Responses:	Certificate ID: Hash Algorithm – Hash algorithm used Issuer Name Hash – Hash sum of the certificate issuer's name Issuer Key Hash – Hash sum of the certificate issuer's public key Serial Number – Certificate's serial number
Cert Status	• **good** – the certificate is not present in CRL • **unknown** – such certificate cannot be found • **revoked** - the certificate is cancelled or revoked;
This Update	[starting date and time on UTC of the validity of the issued CRL, based on

	which the response was generated]
Next Update	[date and time on UTC of a planned CRL update]
OCSP Nonce:	[information, submitted at the request in the Nonce field]
Signature Algorithm:	sha256WithRSAEncryption
Certificate:	[The validation authority's qualified certificate]

7.2.1 PROFILE OF CERTIFYING AUTHORITY "EVROTRUST RSA VALIDATION"

The contents of the status certificate „Evrotrust RSA Validation" of the base certification authority „Evrotrust RSA Root CA" is:

Version	V3	
Serial number	38:00:00:00:09:93:96:2D:78:FF:6E:BA:79:00:00:00:00:00:09	
Signature Algorithm	SHA256RSA	
Valid from	20210317095231Z	
Validit to	20260317100231Z	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust RSA Root CA OCSP
	OU=	OCSP Signing
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	9C:F5:52:24:C8:91:5B:3B:AC:B0:1A:82:C5:8B:F8:06:25:5C:3B:46	
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	74:5C:A1:40:73:2E:1F:E6:F9:3B:BC:AB:A0:A4:A7:54:44:74:4F:70	
OCSP No Revocation Checking	NULL	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl	

Thumbprint SHA1: 0BFA92A3EA5B058792618A270A0B196A18CDF07B

Thumbprint SHA256:

77D7A7B05EC6BEA6AD3C80EFDAB2C0CA769F239821659EE7A86BEBE631217F12

7.2.2 PROFILE OF CERTIFYING AUTHORITY "EVROTRUST RSA QS VALIDATION"

The contents of the status certificate „Evrotrust RSA QS Validation" of the operational certification authority „Evrotrust RSA Operational CA" is:

Version	V3	
Serial number	5E:42:D8:F7:21:03:C4:BC:3F:C1:11:06:A8:D8:9E:DB:9D:3A:4C:3E	
Signature Algorithm	SHA256RSA	
Valid from	20210317111914Z	
Validit to	20260316111914Z	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust RSA Operational CA OCSP
	OU=	OCSP Signing
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	E2:F3:4D:3A:F3:20:8A:71:55:D5:8D:97:FA:BB:73:5C:F5:77:24:E6	
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	7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
OCSP No Revocation Checking	NULL	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	

Thumbprint SHA1: 3AAFAC82D429A697AEDFCCB9CB8C81FF805308CC

Thumbprint SHA256: 10DDCB

60DCB2E600FA2ACE15DC79BEF9A3F2E6E375E2722CDBCE6319DD14968E

7.2.3 PROFILE OF CERTIFYING AUTHORITY "EVROTRUST SERVICES VALIDATION"

The contents of the status certificate „Evrotrust Services Validation" of the operational certification authority „Evrotrust Services CA" 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: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Authority Key Identifier	KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.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://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
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
QCStatements	id-qcs-pkixQCSyntax-v2[i] (oid=1.3.6.1.5.5.7.11.2) id-etsi-qcs-SemanticsId-**Legal** (oid=0.4.0.194121.1.2) id-etsi-qcs-**QcCompliance** (oid=0.4.0.1862.1.1)

	id-etsi-qcs-**QcSSCD** (oid=0.4.0.1862.1.4)	
	id-etsi-qcs-**QcType** (oid=0.4.0.1862.1.6)	id-etsi-qct-**eseal** (oid=0.4.0.1862.1.6.2)

	id-etsi-qcs-**QcPDS** (oid=0.4.0.1862.1.5)	PdsLocations
		PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
		language=en

Thumbprint SHA1: E1CBEE3169AE35A4E3C842B91A962F1B9DD8BFA3

Thumbprint SHA256:

95D9B9BDDF5CD372E84E02AC52A38592ADE3453DC5CE0904AE75E8CA35227705

7.3 PROFILE OF OPERATIONAL CERTIFICATION AUTHORITY „EVROTRUST RSA OPERATIONAL CA“

Version	V3	
Serial number	38 00 00 00 03 4e 8e cb 48 09 25 01 bc 00 00 00 00 00 03	
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	21 май 2016 г. 00:34:35 UTC	
Validit to	21 май 2026 г. 03:44:35 UTC	
Subject	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Subject Key Identifier	7f 3e 64 59 85 2b dd 23 29 c2 01 e7 cb c3 69 c0 87 93 2b 08	
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	

Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Time Stamping (1.3.6.1.5.5.7.3.8) OCSP Signing (1.3.6.1.5.5.7.3.9)
Subject Alternative Name	URL=http://www.evrotrust.com RFC822 Name=ca@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
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=0

7.4 PROFILE OF OPERATIONAL CERTIFICATION AUTHORITY „EVROTRUST SERVICES CA“

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 юли 2019 г. 12:50:59 UTC	
Validit to	10 юли 2029 г. 13:00:59 UTC	
Subject	CN=	Evrotrust Services CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG

Public Key Type/Length	RSA (2048 Bits)
Subject Key Identifier	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
Subject Alternative Name	URL=http://www.evrotrust.com RFC822 Name= servicesca@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
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, 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

7.5 CRL PROFILES

The profile of CRLs is as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 or IETF RFC 5280 as follows:

a) Basic attributes of the list of cancelled and revoked certificates (CRL)

- Version - version of the List;
- Issuer Name – Name of the List issuer (Certification authority);

- Effective Date/This update – date and time of the List (CRL) issuance;
- Next Update - time of the CRL validity. After that time, the certification authority shall immediately issue a new list. During the period of validity, in the event of cancellation/revocation of a certificate, the certification authority automatically issues a new CRL;
- Signature algorithm – identifier of the algorithm for creation of an electronic signature of the CRL;
- Signature hash algorithm – algorithm for the creation of an electronic signature.
- ExpiredCertsOnCRL - an identifier indicating that all certificates, including expired ones, are included in this CRL.

b) Additional attributes to the list of cancelled and revoked certificates

"Authority Key Identifier" – identifier of the certification authority, issuing and signing the List of cancelled and revoked certificates (CRL), contains the meaning of "subjectKeyIdentifier" from the certificate of the certification authority.

c) Format of an element from the list of cancelled and revoked certificates (CRL)

The list of cancelled and revoked certificates (CRL) of the certification authority contains elements of all cancelled certificates. These elements are constant in the List.

The List of cancelled and revoked certificates (CRL) of the certification authority contains an element for each certificate cancelled by the certification authority. This element is temporary in the list until the certificate resumption.

d) Attributes of an element in the list of cancelled and revoked certificates (CRL)

- Serial number - serial number of a cancelled certificate;
- Revocation date - time of the certificate cancellation/revocation;
- CRL Reason Code - code identifying the reason for cancellation/revocation.

e) Indications of the reason for a certificate's cancellation/revocation

- keyCompromise - compromised private key of a Signatory/Creator;
- ACompromise - compromised private key of the Evrotrust operational Certification Authority;
- affiliationChange - changed status of the Signatory to another person – change in the representative power, withdrawal of representative powers, termination of employment, etc.;
- superseded - the certificate has been superseded by another one;
- certificateHold - the certificate is temporarily suspended.

7.5.1 PROFILE OF THE BASE CERTIFICATION AUTHORITY EVROTRUST RSA ROOT CA

Version	V2	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Effective date	[effective date and time under UTC of validity of the issued CRL]	
Next update	[date and time under UTC of planned update of CRL]	
Signature Aagorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70	
CA Version	V0.0	
CRL Number	[order number of CRL]	
Next CRL Publish	[date and time under UTC of planned publishing of the next CRL]	
expiredCertsOnCRL (OID=2.5.29.60)	[UTC date on which the CRL starts to keep revocation status information for expired certificates]	

7.5.2 PROFILE OF THE CRL OPERATIONAL CERTIFICATION AUTHORITY "EVROTRUST RSA OPERATIONAL CA"

Version	V2	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Effective date	[effective date and time under UTC of validity of the issued CRL]	
Next update	[date and time under UTC of planned update of CRL]	
Signature Aagorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=7f 3e 64 59 85 2b dd 23 29 c2 01 e7 cb c3 69 c0 87 93 2b 08	
CA Version	V0.0	
CRL Number	[order number of CRL]	
ExpiredCertsOnCRL	[start date for included certificates]	
Next CRL Publish	[date and time under UTC of planned publishing of the next CRL]	
expiredCertsOnCRL	[UTC date on which the CRL starts to keep revocation status information	

(OID=2.5.29.60)	for expired certificates]

7.5.3 PROFILE OF THE CRL OPERATIONAL CERTIFICATION AUTHORITY „EVROTRUST SERVICVES CA“

Version	V2	
Issuer	CN=	Evrotrust Services CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Effective date	[effective date and time under UTC of validity of the issued CRL]	
Next update	[date and time under UTC of planned update of CRL]	
Signature Algorithm	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	[order number of CRL]	
expiredCertsOnCRL (OID=2.5.29.60)	[UTC date on which the CRL starts to keep revocation status information for expired certificates]	

7.6 PROFILES OF THE USER QUALIFIED CERTIFICATES

a) content of the profile of qualified certificates

In accordance with the X.509 v.3 standard, the electronic certificate is a sequence of the following fields:

- Version: version of the certificate (X.509 v.3);
- SerialNumber: unique identification code of the certificate;
- SignatureAlgorithm: identifier of the algorithm for the electronic signature creation;
- Issuer: distinguished name of the certificate issuer (DN);
- Validity: validity period, described by the date and time of the certificate issuance (notBefore) to the date and time of certificate's expiry (notBefore) (universal coordinated time, presented in Zulu format);
- Subject: distinguished name (DN) of the Signatory/Creator, subject to entry in the certificate;
- SubjectPublicKeyInfo: identifier of the key;
- Signature: identifier of the algorithm for the electronic signature/seal creation, in

accordance with RFC 5280.

b) VERSION

All certificates issued by Evrotrust are in accordance with Version 3 (X.509 v.3).

c) ELIGIBLE EXTENSIONS IN THE FORMAT OF QUALIFIED CERTIFICATES

The values of the extensions are created in accordance with the RFC 5280 recommendation. The function of each extension is determined by the standard value of the respective object identifier (IDENTIFIER):

- Subject Key Identifier - formed by the public key, verified in the certificate as a hash value of the public key;
- Authority Key Identifier - formed as a hash value of the public key of the Evrotrust operational Certification Authority;
- Issuer Alternative Name - includes a URL-string as an alternative name of Evrotrust;
- Basic Constrains – is optional and determines the certificate type;
- Certificate Policy - determines the identifier of the Policy on qualified certificates of qualified electronic signature/seal;
- Key Usage - an attribute setting the restrictions on the certificate usage;
- Extended Key Usage - adds to the meaning of the "Key Usage" attribute and indicates additional and specific applications of the certificate;
- CRL Distribution Point - contains a link to the current CRL of the Evrotrust operating Certification Authority;
- Authority Information Access - contains the URL-address of the OCSP server of the certificate;

Qualified Statements - the attribute contains an instruction that the certificate is qualified and indicates whether the private key is generated and stored on electronic signature creation devices (QSCD).

d) IDENTIFIERS OF ELECTRONIC SIGNATURE/SEAL ALGORITHMS

The attribute "Signature algorithm" identifies the algorithms (cryptographic mechanisms) used.

Evrotrust uses an applicable combination of asymmetrical and hash algorithms: sha256-with-RSA and sha384-with-RSA.

e) NAMING FORMS

The naming forms are described in the "Types of names" part of this document.

f) RESTRICTIONS ON NAMES

The types of restrictions on the names are described in the "Types of names" part of this document.

g) POLICY IDENTIFIER

A qualified certificate issued in accordance with the Evrotrust Policy, which fits into the attribute "Certificate Policy" of the certificate.

h) EXTENSION IDENTIFIER

This identifier ("Extensions") provides a specific information related to the service. For its use at this stage the Practice sets no restrictions.

i) DESIGNATION OF THE QUALIFIED CERTIFICATE

Evrotrust, in the qualified certificate with profile under the X.509 v.3 standard, uses the "Qualified Statements" attribute with identifier: "esi4-qcStatement-1" (OID=0.4.0.1862.1.1).

Evrotrust, in the qualified certificate for qualified electronic signature with profile under the X.509 v.3 standard, uses the "Qualified Statements" attribute with identifiers: "esi4-qcStatement-1" (OID = 0.4.0.1862.1.1) and "esi4-qcStatement-4" (OID=0.4.0.1862.1.4).

Evrotrust, in the qualified certificate with profile under the X.509 v.3 standard, uses the "Certificate Policy" to which the identifier (OID) is assigned with a meaning, as follows:

Qualified Certificate	**Name**	**Identifier (OID) entered in the "Certificate Policy" attribute**
Qualified certificate for a qualified electronic signature of a natural person	Evrotrust Qualified Natural Person Certificate for QES	OID=1.3.6.1.4.1.47272.2.2
Qualified certificate for an attribute qualified electronic signature of a natural person	Evrotrust Qualified Natural Person Attribute Certificate for QES	OID=1.3.6.1.4.1.47272.2.2.1
Qualified certificate for a qualified electronic seal of a legal person/organization	Evrotrust Qualified Legal Person Certificate for QESeal	OID=1.3.6.1.4.1.47272.2.3
Qualified certificate for qualified	Evrotrust Qualified Natural	OID=1.3.6.1.4.1.47272.2.7

electronic signature for natural person	Person Certificate for AES	
Qualified certificate for advanced electronic seal of a legal person/organization	Evrotrust Qualified Legal Person Certificate for AESeal	OID=1.3.6.1.4.1.47272.2.8
Qualified PSD2 certificate – an advanced electronic seal of a legal person/organization	Evrotrust Qualified PSD2 Legal Person Certificate for AESeal	OID=1.3.6.1.4.1.47272.2.8.1
Qualified website authentication certificate for domain	Evrotrust SSL Domain Validated Certificate	OID=1.3.6.1.4.1.47272.2.4.1
Qualified website authentication certificate for organization	Evrotrust SSL Organization Validated Certificate	OID=1.3.6.1.4.1.47272.2.4.2
Qualified website authentication certificate with extended validation	Evrotrust SSL EV Certificate	OID=1.3.6.1.4.1.47272.2.5
Qualified PSD2 website authentication certificate	Evrotrust SSL PSD2 Certificate	OID=1.3.6.1.4.1.47272.2.5.1
Other identifiers (OID), entered in the "Certificate Policy" attribute of the qualified certificates		
QCP-n: Certification policy of the European union (EU) for Qualified certificates, issued to natural persons	qcp-natural	OID=0.4.0.194112.1.0
QCP-l: Certification policy of the European union (EU) for Qualified certificates, issued to legal persons/organizations	qcp-legal	OID=0.4.0.194112.1.1
QCP-n-qscd: Certification policy of the European union (EU) for Qualified certificates, issued to natural persons with a private key, related to the certified public key, located at the QSCD	qcp-natural-qscd	OID=0.4.0.194112.1.2

QCP-l-qscd: Certification policy of the European union (EU) for Qualified certificates, issued to legal persons/organizations with a private key, related to the certified public key, located at the QSCD	qcp-legal-qscd	OID=0.4.0.194112.1.3
QCP-w: Certification policy of the European union (EU) for website authenticity certificate	qcp-web	OID=0.4.0.194112.1.4
OVCP (Organizational Validation Certificate Policy) according to ETSI TS 102 042	ovcp	OID=0.4.0.2042.1.7

j) USING AN IDENTIFIER FOR AN EXTENSION OF THE “CRITICAL” KEY

In practice there is no requirement to use the „CRITICAL CERTIFICATE EXTENSIONS “.

7.6.1 PROFILE OF A QUALIFIED CERTIFICATE FOR A QUALIFIED ELECTRONIC SIGNATURE OF A PHYSICAL PERSON "EVROTRUST QUALIFIED NATURAL PERSON CERTIFICATE FOR QES"

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[starting date and time by UTC of the certificate validity]	
Validit to	[ending date and time by UTC of the certificate validity]	
Subject	C= (countryName)	Country: Two - letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.

	CN= (commonName)	Common name: Selected by the physical person, with which he/she is normally introduced. When it is not selected, the full name of the physical person is entered.
	G= (givenName)	Given name: Physical person name according to the identity document
	S= (surname)	Surname: Physical person surname according to the identity document
		Or
	2.5.4.65= (pseudonym)	Pseudonym: Pseudonym, selected by the physical person
	SERIALNUMBER= (serialNumber)	Physical person identifier (ETSI EN 319 412-1 p.5.1.3), for example: - PNOBG-8310257645 for Civil Identification Number; - PASSBG-12345678 for passport number; - IDCBG-195416023 for identity card number; - TINBG-123434341 for VAT number If the person does not wish to enter his/her national identifier, a client number shall be entered, generated by the provider, to identify the individual if necessary.
	O[i] = (organizationName)	Organization name: Full name of the organization under registration or act of entry by which the physical person is associated.
	2.5.4.97[i] = (organizationIdentifier)	Organization identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 – VAT; - NTRBG-123456789 – UIC (BULSTAT). The national identifier according to the local law of the organization by which the physical person is associated is entered.
	E= (e-mailAddress)	E-mail address of the physical person

<table>
<tr><td>Public Key Type/Length</td><td>RSA (2048 / 3072/ 4096 Bits)</td></tr>
<tr><td>Subject Key Identifier</td><td>[Calculated value for the issued certificate]</td></tr>
<tr><td>Authority Key Identifier</td><td>Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08</td></tr>
<tr><td>CRL Distribution Points</td><td>[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl</td></tr>
<tr><td>Authority Information Access</td><td>[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/EvrotrustRSAOperationalCA.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</td></tr>
<tr><td>Enhanced Key Usage</td><td>Client Authentication (1.3.6.1.5.5.7.3.2)
Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.2
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps
[2]Certificate Policy:
Policy Identifier=0.4.0.194112.1.2</td></tr>
<tr><td>Key Usage (critical)</td><td>Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2) [iii]</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2[i]
(oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-semanticsId-<b>Natural</b>
(oid=0.4.0.194121.1.1)
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>id-etsi-qcs-<b>QcLimitValue</b>[ii]
(0.4.0.1862.1.2)</td><td>[Amount in BGN or EUR]</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>esign</b> (oid=0.4.0.1862.1.6.1)</td></tr>
<tr><td>id-etsi-qcs-<b>QcPDS</b>
(oid=0.4.0.1862.1.5)</td><td>PdsLocations</td></tr>
</table>
</td></tr>
</table>

		PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
		language=en

7.6.2 PROFILE OF A QUALIFIED CERTIFICATE FOR AN QUALIFIED ELECTRONIC SIGNATURE OF A PHYSICAL PERSON "EVROTRUST QUALIFIED NATURAL PERSON CERTIFICATE FOR AES"

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[starting date and time by UTC of the certificate validity]	
Validit to	[ending date and time by UTC of the certificate validity]	
Subject	C= (countryName)	Country: Two - letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Common name: Selected by the physical person, with which he/she is normally introduced. When it is not selected, the full name of the physical person is entered.
	G= (givenName)	Given name: Physical person name according to the identity document
	S= (surname)	Surname: Physical person surname according to the identity document
	Or	
	2.5.4.65= (pseudonym)	Pseudonym: Pseudonym, selected by the physical person

	SERIALNUMBER= (serialNumber)	Physical person identifier (ETSI EN 319 412-1 p.5.1.3), for example: - PNOBG-8310257645 for Civil Identification Number; - PASSBG-12345678 for passport number; - IDCBG-195416023 for identity card number; - TINBG-123434341 for VAT number If the person does not wish to enter his/her national identifier, a client number shall be entered, generated by the provider, to identify the individual if necessary.
	O[i] = (organizationName)	Organization name: Full name of the organization under registration or act of entry by which the physical person is associated.
	2.5.4.97[i] = (organizationIdentifier)	Organization identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 – VAT; - NTRBG-123456789 – UIC (BULSTAT). The national identifier according to the local law of the organization by which the physical person is associated is entered.
	E= (e-mailAddress)	E-mail address of the physical person
Public Key Type/Length	RSA (2048 / 3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for the issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.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/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name:	

<table>
<tr><td></td><td>URL=http://ca.evrotrust.com/ocsp</td></tr>
<tr><td>Enhanced Key Usage</td><td>Client Authentication (1.3.6.1.5.5.7.3.2)
Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=0.4.0.194112.1.0
[2]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.7
[2,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>Key Usage (critical)</td><td>Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2)[iii]</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2[i]
(oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-semanticsId-<b>Natural</b>
(oid=0.4.0.194121.1.1)
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>id-etsi-qcs-<b>QcLimitValue</b>[ii]
(0.4.0.1862.1.2)</td><td>[Amount in BGN or EUR]</td></tr>
<tr><td>id-etsi-qcs-<b>QcType</b>
(oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-<b>esign</b> (oid=0.4.0.1862.1.6.1)</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>
</td></tr>
</table>

7.6.3 PROFILE OF A QUALIFIED CERTIFICATE FOR A QUALIFIED ELECTRONIC STAMP OF A LEGAL PERSON "EVROTRUST QUALIFIED LEGAL PERSON CERTIFICATE FOR QESEAL"

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[starting date and time by UTC of the certificate validity]	

Validit to	[ending date and time by UTC of the certificate validity]	
Subject	C= (countryName)	Country: Two - letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Name of the legal entity/the organization
	O= (organizationName)	Name of the legal entity/the organization: Full name of the organization under registration or act of entry.
	2.5.4.97= (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 – VAT; - NTRBG-123456789 – UIC (BULSTAT). The national identifier according to the local law of the legal entity by which the physical person is associated is entered.
	E= (e-mailAddress)	Legal entity e-mail address
Public Key Type/Length	RSA (2048 / 3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for the issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.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/EvrotrustRSAOperationalCA.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	
Enhanced Key	Client Authentication (1.3.6.1.5.5.7.3.2)	

<table>
<tr><td>Usage</td><td>Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.3
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps
[2]Certificate Policy:
Policy Identifier=0.4.0.194112.1.3</td></tr>
<tr><td>Key Usage (critical)</td><td>Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2) [iii]</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2
(oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-<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>id-etsi-qcs-<b>QcLimitValue</b>[ii]
(0.4.0.1862.1.2)</td><td>[Amount in BGN or EUR]</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>
</td></tr>
</table>

7.6.4 PROFILE OF QUALIFIED CERTIFICATE FOR „EVROTRUST QUALIFIED LEGAL PERSON CERTIFICATE FOR AESEAL"

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[starting date and time by UTC of the certificate validity]	
Validit to	[ending date and time by UTC of the certificate validity]	

Subject	C= (countryName)	Country: Two - letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Name of the legal entity/the organization
	O= (organizationName)	Name of the legal entity/the organization: Full name of the organization under registration or act of entry.
	2.5.4.97= (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 – VAT; - NTRBG-123456789 – UIC (BULSTAT). The national identifier according to the local law of the legal entity by which the physical person is associated is entered.
	E= (e-mailAddress)	Legal entity e-mail address
Public Key Type/Length	RSA (2048 / 3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for the issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.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/EvrotrustRSAOperationalCA.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	
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	

<table>
<tr><td></td><td></td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=0.4.0.194112.1.1
[2]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.8
[2,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>Key Usage (critical)</td><td>Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2) [iii]</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-<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>id-etsi-qcs-<b>QcLimitValue</b>[ii] (0.4.0.1862.1.2)</td><td>[Amount in BGN or EUR]</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>
</td></tr>
</table>

7.6.5 PROFILE OF QUALIFIED PSD2 LEGAL PERSON CERTIFICATE FOR AESEAL „EVROTRUST QUALIFIED PSD2 LEGAL PERSON CERTIFICATE FOR AESEAL"

The certificate is issued for the purpose of authenticating a legal entity/organization associated as a PSD (PSP) under PSD2 regulation. It has the character of a Qualified certificate for advanced electronic seal according to the Regulation (EU) No 910/2014 and is used to electronically sign documents / data to fulfil PSD2 requirements.

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA

	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Validit to	[UTC end date and time of certificate validity]	
Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Legal entity/organisation name:
	O= (organizationName)	Legal entity/organisation name: Full name under the registration or act of registration of the legal entity.
	2.5.4.97= (organizationIdentifier)	Legal entity identifier (ETSI TS 119 495 p.5.2.1), for example: - PSDES-BDE-3DFD21 (PSD 2). Enter the national identifier according to the local law of the legal entity with which the natural person is associated.
Public Key Type/Length	RSA (2048 / 3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	
Authority Information Access	1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:	

<table>
<tr><td></td><td>URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.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</td></tr>
<tr><td>Enhanced Key Usage</td><td>Client Authentication (1.3.6.1.5.5.7.3.2)
Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=0.4.0.194112.1.1
[2]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.8.1
[2,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>Key Usage (critical)</td><td>Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2) [iii]</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-<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>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>
<tr><td>id-etsi-<b>psd2</b>-qcStatement (oid=0.4.0.19495.2)</td><td>rolesOfPSP
roleOfPspOid = 0.4.0.19495.1.1/2/3/4
roleOfPspName = PSP_AS/PSP_PI/PSP_AI/PSP_IC
nCAName= Full name of the NCA
nCAId= NCA abbreviated unique identifier</td></tr>
</table>
</td></tr>
</table>

7.6.6 PROFILE OF A QUALIFIED ORGANIZATION WEBSITE CERTIFICATE OF AUTHENTICITY „EVROTRUST SSL ORGANIZATION VALIDATED CERTIFICATE“

Version	V3
Serial number	[serial number]
Signature Algorithm	SHA256RSA

Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Validit to	[UTC end date and time of certificate validity]	
Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Domain name, IP or Resource name
	O = (organizationName)	Name of the person: Full name under the registration or act of registration of the legal entity with which the natural person is associated.
	OU[1]= (organizationalUnitName)	Organizational unit name
	2.5.4.97[1] = (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 – VAT; - NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity.
	ST[1] = (stateOrProvinceName)	Legal entity region/state
	L[1] = (localityName)	Legal entity locatity/citi
Public Key Type/Length	RSA (2048 / 3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.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/EvrotrustRSAOperationalCA.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
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	DNS Name=[Domain name or IP]
Certificate Policies	[1]Certificate Policy: Policy Identifier=0.4.0.2042.1.7 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.4.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)

7.6.7 PROFILE OF A QUALIFIED CERTIFICATE FOR AUTHENTICITY OF WEBSITE WITH EXTENDED VALIDATION „EVROTRUST SSL EV CERTIFICATE“

The certificate is issued for the purposes of authenticating a website specifically related to the natural or legal person. The certificate has the character of a qualified website certificate within the meaning of the Regulation and is used to create confident visitor that the website is a real and legitimate subject. Through technology, reliable connectivity is secured through a secure data exchange protocol.

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Validit to	[UTC end date and time of certificate validity]	

Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166. Specifies a general context in which other attributes of Subject fieldare to be understood.
	CN= (commonName)	Domain name, IP or Resource name
	O[i] = (organizationName)	Name of the legal entity: Full name under the registration or act of registration of the legal entity.
	2.5.4.97[i] = (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: • VARBG-123456789 – VAT; • NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity.
Public Key Type/Length	RSA (2048 / 3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.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/EvrotrustRSAOperationalCA.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	
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
Subject Alternative Name	DNS Name=[Domain name or IP]	

Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4	
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)	
QCStatements	id-qcs-pkixQCSyntax-v2[i] (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId-**Legal** (oid=0.4.0.194121.1.2)
	id-etsi-qcs-**QcCompliance** (oid=0.4.0.1862.1.1)	
	id-etsi-qcs-**QcLimitValue**[ii] (oid=0.4.0.1862.1.2)	[Amount in BGN or EUR]
	id-etsi-qcs-**QcType** (oid=0.4.0.1862.1.6)	id-etsi-qct-**web** (oid=0.4.0.1862.1.6.3)

	id-etsi-qcs-**QcPDS** (oid=0.4.0.1862.1.5)	PdsLocations
		PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
		language=en

7.6.8 PROFILE OF A QUALIFIED CERTIFICATE FOR AUTHENTICITY OF WEBSITE „EVROTRUST SSL PSD2 CERTIFICATE“

The certificate is issued for the purpose of authenticating a PSD2 related PSP2 website. Used to meet PSD2 requirements. It has the character of a qualified website certificate within the meaning of Regulation (EU) No 910/2014 and is used to create a confident visitor that the website is a real and legitimate subject. Through technology, reliable connectivity is secured through a secure data exchange protocol.

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC

	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Validit to	[UTC end date and time of certificate validity]	
Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Legal entity/organisation name:
	O[i] = (organizationName)	Legal entity/organisation name: Full name under the registration or act of registration of the legal entity.
	2.5.4.97[i] = (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: • VARBG-123456789 - VAT; • NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity.
Public Key Type/Length	RSA (2048 / 3072 / 4096 Bits)	
Subject Key Identifier	[Calculated value for issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.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/EvrotrustRSAOperationalCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name:	

<table>
<tr><td></td><td>URL=http://ca.evrotrust.com/ocsp</td></tr>
<tr><td>Enhanced Key Usage</td><td>Client Authentication (1.3.6.1.5.5.7.3.2)
Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
<tr><td>Subject Alternative Name</td><td>DNS Name=[Domain name or IP]</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.5.1
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps
[2]Certificate Policy:
Policy Identifier=0.4.0.194112.1.4</td></tr>
<tr><td>Key Usage (critical)</td><td>Digital Signature (Bit 0), Key Encipherment (Bit 2)</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-<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>id-etsi-qcs-<b>QcType</b> (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-<b>web</b> (oid=0.4.0.1862.1.6.3)</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>
<tr><td>id-etsi-<b>psd2</b>-qcStatement (oid=0.4.0.19495.2)</td><td>rolesOfPSP
roleOfPspOid = 0.4.0.19495.1.1/2/3/4
roleOfPspName = PSP_AS/PSP_PI/PSP_AI/PSP_IC
nCAName= Full name of the NCA
nCAId= NCA abbreviated unique identifier</td></tr>
</table>
</td></tr>
</table>

7.6.9 PROFILE OF QUALIFIED NATURAL PERSON ATTRIBUTE CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE "EVROTRUST QUALIFIED NATURAL PERSON ATTRIBUTE CERTIFICATE FOR QES“

The qualified attribute certificate for a qualified electronic signature of a physical person is issued under the same conditions as the qualified certificate for a qualified electronic signature of a physical person, but it differs in terms of type and volume of the data certified in it. It is used to identify the person in front of the Relying Party.

<table>
<tr><td>Version</td><td colspan="2">V3</td></tr>
<tr><td>Serial number</td><td colspan="2">[serial number]</td></tr>
<tr><td>Signature Algorithm</td><td colspan="2">SHA256RSA</td></tr>
<tr><td rowspan="5">Issuer</td><td>CN=</td><td>Evrotrust RSA Operational CA</td></tr>
<tr><td>OU=</td><td>Qualified Operational CA</td></tr>
<tr><td>O=</td><td>Evrotrust Technologies JSC</td></tr>
<tr><td>organizationIdentifier (2.5.4.97)= (2.5.4.97)</td><td>NTRBG-203397356</td></tr>
<tr><td>C=</td><td>BG</td></tr>
<tr><td>Valid from</td><td colspan="2">[starting date and time by UTC of the certificate validity]</td></tr>
<tr><td>Validit to</td><td colspan="2">[ending date and time by UTC of the certificate validity]</td></tr>
<tr><td rowspan="9">Subject</td><td>C=
(countryName)</td><td>Country: Two - letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.</td></tr>
<tr><td>CN=
(commonName)</td><td>Common name: Full name of the physical person in Latin by identity document</td></tr>
<tr><td>G=
(givenName)</td><td>Given name: Name of the physical person in Latin by identity document</td></tr>
<tr><td>S=
(surname)</td><td>Surname: Surname of the physical person in Latin by identity document</td></tr>
<tr><td>name*=
(id-at-name)</td><td>Full name: Full name of the physical person in Cyrillic by identity document.</td></tr>
<tr><td>SERIALNUMBER=
(serialNumber)</td><td>National identifier of the physical person in conformity to ETSI EN 319 412-1 т.5.1.3, for example: PNOBG-8310257645 for Civil Identification Number or another identifier which is associated with the physical person.</td></tr>
<tr><td>gender*=
(id-pda-gender)</td><td>Gender of the physical person at birth: M or F (male/female)</td></tr>
<tr><td>dateOfBirth*=
(id-pda-dateOfBirth)</td><td>Birth date with accuracy to days in ZULU format, for example: 19831231120000Z</td></tr>
<tr><td>description*=
(id-at-description)</td><td>Date from the machine-readable sections of the physical person identity document (Machine-readable passport)
<table>
<tr><th>Position</th><th>Length</th><th>Symbol</th><th>Meaning</th></tr>
<tr><td>1</td><td>1</td><td>alpha</td><td>I, A or C</td></tr>
<tr><td>2</td><td>1</td><td>alpha <</td><td>Type: It is filled in at the discretion of the issuing country or authority. IP</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>for passport and ID for national identity card are most often used.</td></tr>
<tr><td>3-5</td><td>3</td><td>alpha &lt;</td><td>Code of the country, issuing the identity document in conformity to (ISO 3166-1 alpha-3 code with modifications)</td></tr>
<tr><td>6-14</td><td>9</td><td>alpha num &lt;</td><td>Number of identity document</td></tr>
<tr><td>15</td><td>1</td><td>num &lt;</td><td>Control number of the digits 6-14</td></tr>
<tr><td>16</td><td>1</td><td>:</td><td>Divider</td></tr>
<tr><td>17</td><td>6</td><td>num</td><td>Year, month and date (YYMMDD) to which the identity document is valid</td></tr>
<tr><td>18</td><td>1</td><td>:</td><td>Divider</td></tr>
<tr><td>19</td><td>6</td><td>num</td><td>Year, month and date (YYMMDD) when the identity document is issued</td></tr>
</table>
For example:
IDBGR**641020223**4**:**201013:251013
</td></tr>
<tr><td>Public Key Type/Length</td><td colspan="2">RSA (2048 / 3072/ 4096 Bits)</td></tr>
<tr><td>Subject Key I</td><td colspan="2">[Calculated value for the issued certificate]</td></tr>
<tr><td>Authority Key Identifier</td><td colspan="2">Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08</td></tr>
<tr><td>CRL Distribution Points</td><td colspan="2">[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.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://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.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</td></tr>
<tr><td>Enhanced Key Usage</td><td colspan="2">Client Authentication (1.3.6.1.5.5.7.3.2)
Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
</table>

Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.2	
Key Usage (critical)	Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2) [iii]	
QCStatements	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-semanticsId-**Natural** (oid=0.4.0.194121.1.1)
	id-etsi-qcs-**QcCompliance** (oid=0.4.0.1862.1.1)	
	id-etsi-qcs-**QcLimitValue**[ii] (0.4.0.1862.1.2)	[Amount in BGN or EUR]
	id-etsi-qcs-**QcSSCD** (oid=0.4.0.1862.1.4)	
	id-etsi-qcs-**QcType** (oid=0.4.0.1862.1.6)	id-etsi-qct-**esign** (oid=0.4.0.1862.1.6.1)

	id-etsi-qcs-**QcPDS** (oid=0.4.0.1862.1.5)	PdsLocations
		PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
		language=en

**Fields marked with an asterisk may not be present in the certificate*

7.6.10 PROFILE OF QUALIFIED CERTIFICATE FOR DOMAIN WEBSITE AUTHORITY „EVROTRUST SSL DOMAIN VALIDATED CERTIFICATE“

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Validit to	[UTC end date and time of certificate validity]	

Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Domain name, IP or Resource name
Public Key Type/Length	RSA (2048 / 3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.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/EvrotrustRSAOperationalCA.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	
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	
Subject Alternative Name	DNS Name=[Domain name or IP]	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)	

7.7 QUALIFIED TIME STAMP SIGNING UNIT CERTIFICATE PROFILE

The qualified Time Stamp Authority (TSA) signs the time stamp requests using its time stamp signing units (TSU).

The profile of the “Evrotrust TSA” signing unit certificate is:

Version	V3
Serial number	3FF1A51525B082F969C00FE1688A3D612F7B43B7
Signature Algorithm	SHA256RSA

Valid from	Jan 18 07:55:31 2024 GMT	
Valid to	Jan 16 07:55:30 2029 GMT	
Issuer	CN=	Evrotrust Services CA
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier(2.5.4.97)	NTRBG-203397356
	C=	BG
Subject	CN=	Evrotrust Timestamp TSU 2024
	O=	Evrotrust Technologies JSC
	OrganizationIdentifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key	RSA(2048 Bits)	
Subject Key Identifier	C4728DB862587E9B47187524BEB149029710CD35	
Key Usage (critical)	Digital Signature, Non Repudiation	
Extended keyUsage (critical)	Time Stamping (1.3.6.1.5.5.7.3.8)	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Authority Key Identifier	KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E	
Subject alternative name (not critical)	URL=http://ts.evrotrust.com/tsa	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.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://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	
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None	
QCStatements	id-qcs-pkixQCSyntax-v2[i]	id-etsi-qcs-SemanticsId-**Legal**

	(oid=1.3.6.1.5.5.7.11.2)	(oid=0.4.0.194121.1.2)
	id-etsi-qcs-**QcCompliance** (oid=0.4.0.1862.1.1)	
	id-etsi-qcs-**QcSSCD** (oid=0.4.0.1862.1.4)	
	id-etsi-qcs-**QcType** (oid=0.4.0.1862.1.6)	id-etsi-qct-**eseal** (oid=0.4.0.1862.1.6.2)

	id-etsi-qcs-**QcPDS**
	(oid=0.4.0.1862.1.5)
		PdsLocations
		PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
		language=en

Thumbprint (SHA1): BBF7D2530AEAFB93C4DAAECBFB834747D677A1E4

Thumbprint (SHA256):

C09ACE24529828CAF1019D93FF3F684E15D1FB3F16C3BD3BA6DA0ACEA5938E2A

8. AUDIT

The audits conducted in Evrotrust concern the information data processing and key procedures management. They aim to control the „Certification practice statement

for qualified certification services" to the extent it is compatible with the integrated management system that includes the requirements of IEC 27001, ISO 9001, ISO 22301, ISO/IEC 20000-1, Regulation (EC) No 910/2014 and the internal management decisions and measures. The conducted audits of Evrotrust apply to all Certification Authorities belonging to the basic Certification Authority, the Registration Authority, as well as other elements of the public key infrastructure, such as an OCSP server.

Evrotrust annually conducts at least one internal audit.

Evrotrust is a subject of audit at least once every 24 months by a Conformity Assessment Body. The purpose of the audit is to confirm that Evrotrust, as a qualified certification services provider and the qualified certification services provided by it, meet the requirements set out in Regulation (EU) No 910/2014. The provider shall submit to the Supervisory Body the relevant conformity assessment report within three working days of receiving it.

The Supervisory Body may at any time conduct an audit or request that a Conformity Assessment Body performs a conformity assessment of Evrotrust.

8.1 AUDIT FREQUENCY

The Evrotrust management appoints periodic checks on the current activity compliance with the established Certificate Policy and Certification Practice Statement regarding the operation of Evrotrust.

The Evrotrust management carries out constant operational control for the accurate execution of the instructions at work given by Evrotrust personnel.

8.2 QUALIFICATION OF VERIFIERS

External audit is conducted by an accredited and independent of Evrotrust Conformity assessment body. Auditor accreditation and competence system are specified in Regulation (EC) No 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 and is regulated by ISO/IEC 17065:2012: Conformity assessment - Requirements for bodies certifying products, processes and services.

External inspection by a supervisory body is carried out at any time by authorized employees of the Supervisory body - the Communications Regulation Commission.

The internal audit is performed by Evrotrust employees with the necessary experience and qualification.

For the purposes of auditing, Evrotrust has hired and authorized employees who possess the necessary technical knowledge related to public key infrastructure, with the reliable and secure operation of the technology system, information security, as well as the presence of a large practical experience in auditing.

8.3 VERIFIERS' RELATIONSHIP TO EVROTRUST

Verifiers must be independent, not directly or indirectly related to, and have no conflict of interest with Evrotrust.

The relations between Evrotrust and an external verifier are governed by a contract.

8.4 AUDIT SCOPE

The inspection by the Supervisory body covers the statutory requirements for the activities of Evrotrust according to the applicable legislation in the sector of qualified certification services.

The audit by the Conformity Assessment Body covers the entire Evrotrust operation for the provision of qualified certification services and implementation of all standards and standardization documents related to Regulation (EU) No 910/2014: Documentation; Archives; Information data related to the issuance and management of qualified certificates; Physical and information security and reliability of the technological system and management; Certification Authorities.

The scope of internal audits includes: Verification of the provider's activity and its compliance with the Certificate Policy and Certification Practice Statement; comparison of the practices and procedures outlined in this document with their practical realization in the implementation of the Evrotrust operation; verification of the activity of the Registration Authority; other circumstances, facts and activities related to the Evrotrust infrastructure, at the discretion of the Evrotrust management.

8.5 ACTIONS TAKEN AS A RESULT OF THE AUDIT CONDUCTED

The reports of internal and external audits are submitted to Evrotrust.

The report of the Conformity Assessment Body shall be submitted to the Supervisory Authority within 3 (three) days of its handing over to the Evrotrust management.

Based on the assessments made in the report, Evrotrust Management shall outline measures and deadlines to remedy the identified gaps and inconsistencies.

Evrotrust personnel undertakes specific actions for their removal within the specified deadlines.

8.6 AUDIT RESULTS STORAGE

The results of the performed internal and external audits are properly kept in the Evrotrust archive.

The certification document received by the Conformity Assessment Body may be posted on the Evrotrust website.

9. OTHER BUSINESS CONDITIONS AND LEGAL ASPECTS

9.1 PRICES AND FEES

Evrotrust maintains the document "Tariff of Certification, Information, Cryptographic and Consultancy Services" on its website at: https://www.evrotrust.com.

The Provider has the right to unilaterally change the Tariff at any time during the term of

Contract, and shall notify the Signature Owner/Creator of a seal by publishing the changes on its website.

The change shall be effective for the Signature Owner/Creator of a seal on the day following the day of publication.

Within 5 (five) days from the date of the change, and as far as an increase in the price has occurred, the Signature Owner/Creator of a seal is entitled to unilaterally terminate the Contract by giving a written notice to Evrotrust, as from the date of expiry of the last certificate. In this case, the contract is deemed to have been canceled as of the date of the change and the remuneration paid under the contract for the use of the services shall not be refundable. In the absence of a notice of termination, it is considered that the Signature Owner/Creator of a seal agrees to the change.

The change in the remunerations may not affect remunerations already paid.

9.1.1 FEES

The contract value may include one or more of the following fees:

- fee for the issuance and maintenance of a qualified certificate;
- fee for renewal of a qualified certificate;
- fee for consultations and technological assistance made at the request of the Signature Owner/Creator of a seal;
- price for equipment purchased or leased by Evrotrust;
- fee for personalization of physical media;
- for performing remote signatures;
- fee for performing remote authentication;
- fees related to the secure delivery of electronic messages;
- other fees for qualified certification services provided.

Fees and amounts payable shall be paid to Evrotrust in the amounts, according to the Tariff of Qualified Certification, Information, Cryptographic and Consultancy Services provided by Evrotrust and within deadlines in manner as specified in the Contract and its annexes thereto.

As far as there is an agreed advance or subscription fee for the use of a service, it is shall not be refundable if the Signature Owner/Creator of a seal has not consumed the service provided during the relevant period to which the advance or subscription fee relates.

The price does not include the amounts accrued by telecommunications companies in connection with their services used by the Signature Owner/Creator of a seal for the purposes of the services provided by Evrotrust. These shall be payable entirely by the Signature Owner/Creator of a seal to the relevant telecommunications company. The Provider shall not be held liable and responsible for the payment of these amounts.

All costs and fees for the transfer of the amounts due on the account of Evrotrust are at the expense of the User.

9.1.2 FEES FOR CERTIFICATION, CRYPTOGRAPHIC, INFORMATION AND CONSULTANCY SERVICES

For the services to provide and use Qualified Certificates and related services, a due amount shall be paid when requesting the service. In the other cases, the payment shall be made within 10 days of receipt of the invoice or according to the contract concluded.

The services related to the provision of technological assistance and consultancy for the construction and maintenance of an infrastructure and information security solutions shall be charged on a „man-hour" basis and shall be paid on the basis of a bilaterally signed protocol for the work performed. The prices of the hourly rate in the annexed Tariff are valid within the established working time. When working outside the established working time, the prices shall be increased by an appropriate percentage, according to the Tariff.

The service "Issuance of Qualified Electronic Time-stamps" at an agreed service level shall be paid according to the contractual terms.

The cost of equipment purchased or leased by Evrotrust shall be negotiated and shall be due under the terms of the contract. The legal relationship between Evrotrust and the Signature Owner/Creator of a seal shall be governed by the general rules of the Sale contract, respectively the Lease contract.

In case of delay of payments after the agreed term, the User shall owe to Evrotrust the statutory interest for the period until the final payment of the amounts due.

The use of documents published on the website of Evrotrust is free of charge. For recording and delivery of these documents on a physical medium, the cost of this medium and the courier charges shall be paid.

9.1.3 INVOICING

The Provider shall issue an invoice to the User for services provided.

Failure to receive an invoice does not relieve the User from its obligation to pay the due fees within the agreed deadlines.

All amounts due under the Contract shall be paid by the User in cash or by bank transfer. Payment by bank transfer shall be deemed to be made after the bank account of Evrotrust is credited with the full amount due.

All bank commissions, fees and expenses in connection with the bank transfers shall be borne by the User.

9.1.4 RETURN OF CERTIFICATE AND RECOVERY OF PAYMENT

A Signature Owner/Creator of a seal can object to the inaccuracy or incompleteness in the contents of a certificate within 3 days after its publication in the certificates register.

If the cause of the false content of the certificate lies with the Registration Authority, Evrotrust shall terminate the certificate and shall issue a new one free of charge, with a correct content, or shall recover the payment made for the terminated certificate with the false content.

If the cause of the false content of the certificate is incorrect presentation of data by the Signature Owner/Creator of a seal, Evrotrust shall terminate the certificate and shall not recover the payment made. Evrotrust may issue a new certificate with correct content, to the User's expense.

The User may refuse to accept a qualified certificate issued with true content. In this case, Evrotrust shall terminate it immediately, without recovering the payment made.

9.1.5 FREE SERVICES

The Provider shall provide free registration and information services related to the use of the Public Register/storage, as follows:

- check-up of an electronic signature certificate published in the certificates register and on the web site;
- validity check-up of an issued certificate;
- check-up of the status of a certificate in real time;
- certificate for time of presented content/electronic statement without Service Level Agreement;

- download a current Certificate Revocation List (CRL) and access to CRL archive;
- download the operating certificates of Evrotrust;
- download the public documents of Evrotrust;
- other services.

9.2 FINANCIAL RESPONSIBILITIES

Evrotrust shall be responsible for the certification services provided to the users who rely on the certifications.

Evrotrust shall be liable if the damages are due to his fault or to the parties to whom it has assigned the job.

If Evrotrust acknowledges and agrees that damages have occurred, it shall undertake to pay the damages. The maximum payment limit may not exceed the amount of the damages.

9.2.1 INSURANCE OF ACTIVITIES

Evrotrust conclude compulsory insurance of its activity as a provider of qualified trust services. With regard to the risk of liability for damages in accordance with Article 13 of Regulation (EU) No. 910/2014, Evrotrust shall conclude appropriate liability insurance, in accordance with national law. The compulsory insurance shall be concluded for a continuous period and renewed annually. Subject of the insurance shall be the liability of Evrotrust to perform its activity according to the requirements of the applicable legislation. The compulsory insurance shall cover the liability of Evrotrust to users and relying parties for material and non-material damage within the limits specified in the applicable legislation. Upon occurrence of an event that may result in claiming damage covered by the insurance, the person concerned must notify Evrotrust and the insurer in writing within 7 days after becoming aware of the event. The insurance coverage for non-material and/or material damage suffered by a signature owner/creator shall not exceed the amount established by the national legislation.

9.2.2 INSURANCE COVERAGE

The insurance coverage for any non-material and/or material damage suffered by a Signature Owner/Creator of a seal shall not exceed the amount established by the national legislation.

The insurance shall not cover cases of waiver of responsibility, in particular for damages caused by:

- non-compliance of a Signature Owner/Creator of a seal;
- compromise or loss of private key of a Signature Owner/Creator of a seal due to the failure to exercise the due care to protect the key during use;
- non-compliance with requirements to verify the validity of the electronic signature/seal and the Qualified Certificate by a Relying Party;
- force majeure and other circumstances beyond the control of Evrotrust.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Evrotrust ensures that the collection, processing and storage of information during its activity as a provider of qualified certification services is in accordance with the national legislation.

Evrotrust ensures that the Relying parties have access only to the information that is available in the certificates register and on the provider's web site.

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

Confidential Information for Signature Owner/Creator of a seal is the information which is not included in the issued certificates and the Certificate Revocation List (CRL). It constitutes personal data within the meaning of the Law for Protection of Personal Data (LPPD).

The confidential information is collected by Evrotrust only to the extent necessary for the purposes of issuance and maintenance of the certificates.

The confidential information may not be disclosed to third parties without the explicit consent of the Signature Owner/Creator of a seal, except in cases where the Provider is required by law.

The provider may collect additional information that is also not included in the certificates but is used for the purpose of the qualitative maintenance of the qualified certification services.

Confidential information shall be kept on site, access to which shall be restricted and limited only to persons of Evrotrust personnel authorized to operate the data, and shall be disclosed only after the explicit consent of the Signature Owner/Creator of a seal except in cases where the Provider is obliged by law.

Journal entries and logs from the system of Evrotrust shall be regarded as confidential information and shall be protected from unauthorized access and impact.

9.3.2 NON-CONFIDENTIAL INFORMATION

Non-confidential is any information contained in the certificates register regarding the Qualified Certificates issued, as well as in the published up-to-date Certificate Revocation List (CRL) and in the archive copies of this list.

The following information in the provider's web site is available to the public:

- Certificate Policy and Certification Practice Statement;
- a template of Contract between Evrotrust and the users;
- price list of services provided by Evrotrust;
- user guidelines;
- Contact addresses with the Registration Authority and the Certification Authority;
- user certificates (only after user approval);
- Certificate Revocation List (CRL);
- excerpts from reports (certification document) from the Conformity Assessment Body or other authorized body (as detailed as possible).

The published reports shall inform the public about:

- the scope of the audit;
- the overall assessment for the audit;
- the degree of implementation of the recommendations.

9.3.3 PROTECTION OF CONFIDENTIAL INFORMATION

The Provider and the Signature Owner/Creator of a seal are not allowed to disseminate or allow dissemination of information made known to them during or in connection with their obligations under the Contract, including payments, without the prior written permission of the other Party.

9.4 PRIVACY OF PERSONAL DATA

As a Personal Data Administrator, Evrotrust strictly respects the confidentiality and non-dissemination requirements of the personal data of the Signature Owner/Creator of a seal that have come to his knowledge as Qualified Certification Services Provider.

Evrotrust takes appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of personal data. Evrotrust protects the confidentiality and integrity of registration data, especially when exchanged with the user/subject or between the distributed system components of Evrotrust. As a data administrator, Evrotrust strictly observes the requirements for confidentiality and non-disclosure of personal data of signature owners/creators, which became known to it during the performance of its activity as a provider of qualified trust services. Evrotrust ensures that personal data are collected, stored and processed in accordance with the Personal Data Protection Act and REGULATION (EU) 2016/679 General Data Protection Regulation (GDPR). Evrotrust collects such amount of information that is proportionate to its purpose and use. Every user gives their content to the processing of their personal data. This consent is declared by signing a trust services Agreement. Personal data are used only in relation to the provision of trust services which means that only data that are adequate, relevant and not excessive for providing online access to the services are collected. Personal data are protected in accordance with the confidentiality rules contained in the Privacy Policy of Evrotrust.

9.4.1 PRIVACY STATEMENT

Personal data provided to Evrotrust are stored and processed in accordance with the Law for Protection of Personal Data and Regulation (EU) 2016/679 General Data Protection Regulation (GDPR). Evrotrust collects a quantity of information in proportion to its intended purpose and use. Each user gives consent for the processing of their personal data. This consent is made by signing the Certification Services Contract.

Personal data is only used in connection with the provision of the certification services.

Personal data is protected in accordance with the confidentiality rules contained in Evrotrust security policy.

9.4.2 INFORMATION TREATED AS PERSONAL

Any user information that is not publicly available through the content of the issued certificates, provider's web site, or online by the Certificate Revocation List (CRL) and OCSP shall be treated as personal.

9.4.3 INFORMATION THAT IS NOT CONSIDERED PERSONAL

All the information disclosed in the certificates is considered to be non-personal, unless expressly provided otherwise in the Law for Protection of Personal Data and Regulation (EU)

2016/679 General Data Protection Regulation (GDPR).

9.4.4 RESPONSIBILITY FOR THE PROTECTION OF PERSONAL DATA

Evrotrust and the Registration Authority, which receive confidential information, guarantee the protection of personal data to the users. Evrotrust does not allow compromise and disclosure of personal data to third parties. Providing access to personal information is only in accordance with the requirements of the Law for Protection of Personal Data and Regulation (EU) 2016/679 General Data Protection Regulation (GDPR).

9.4.5 CONSENT FOR THE USE OF PERSONAL DATA

Unless otherwise specified in the "Certification Practice Statement for Qualified Certification Services", the applicable privacy rules (except in the case of an agreement) require that personal data shall not be used without the consent of the Signature Owner/Creator of a seal except in the cases provided for by law.

9.4.6 OTHER CIRCUMSTANCES FOR DISCLOSURE OF INFORMATION

The Certification Practice Statement for Qualified Certification Services does not indicate any other circumstances in this regard.

9.5 INTELLECTUAL PROPERTY RIGHTS

Various data included in the Evrotrust qualified certificates or published in the certificates register and on the Evrotrust's web site are subject to intellectual property rights and other tangible and intangible rights.

Relations on the occasion of these rights between Evrotrust and the other participants in the infrastructure of Evrotrust, such as external Registration Authorities and other shall be governed by contract.

All qualified certificates issued by Evrotrust shall be subject to the copyright of Evrotrust.

All rights on trademarks used by Evrotrust (e.g., Evrotrust®), as well as the trade names contained in the certificates used by the Signature Owner/Creator of a seal shall be retained by their Signature Owners/Creators of a seal and shall be used only for the purposes of the Certification Services provided.

Key pair corresponding to the certificates issued by Evrotrust, as well as the corresponding classified material shall be subject to the rights of Evrotrust rights, regardless of the ownership over the physical media of the keys.

9.5.1 RIGHT TO OWNERSHIP OF DATA IN QUALIFIED CERTIFICATES

Evrotrust shall retain all intellectual property rights of the data included in the Qualified Certificates.

9.5.2 RIGHT TO OWNERSHIP OF NAMES AND TRADEMARKS

Evrotrust owns a registered trademark consisting of a graphic sign and an inscription which is the following logo:

The logo is a registered trademark of Evrotrust and can not be used by other parties without the prior written approval of Evrotrust.

All users reserve the intellectual property right to a trademark, service mark, or trade name contained in each Qualified Certificate issued.

Intellectual property right is the unique name (DN) within each certificate issued to Signature Owners/Creators of a seal.

9.5.3 OWNERSHIP OF A KEY PAIR

The user key pair and the connected to the public key qualified certificate issued by Evrotrust, as well as the corresponding classified material, are ownership of Evrotrust, regardless of the ownership of the physical environment in which the keys are stored and protected.

The Certification Authorities are owned by Evrotrust.

9.6 GENERAL CONDITIONS

This part of Certification practice statement for qualified certification services describes the obligations, guarantees and liability of Evrotrust, the Registration Authority, the users and the relying parties. The rights, obligations and due diligence of the users and the relying parties are settled. The obligations and liability of the users and Evrotrust are settled by contractual agreements. Relationships with relying parties are governed by common delict law.

Contracts for the provision of certification services should be concluded in written or electronic form, subject to the provisions of Regulation (EC) No 910/2014, Regulation (EU) No 2016/679 and the applicable legislation in the Republic of Bulgaria.

9.6.1 LIABILITIES, RESPONSIBILITY, AND GUARANTEES OF EVROTRUST

Evrotrust guarantees that it carries out its activities as:

- strictly complies with the terms of this document, the requirements of Regulation (EC) No 910/2014, Regulation (EU) No 2016/679 and the national legislation in the performance of its activity as a Provider of Qualified Certification Services;
- the services provided do not infringe the copyrights and licensed rights of third parties;
- uses technical equipment and technologies that ensure reliability of the systems and the technical and cryptographic security in the process implementation, including also a safe and secure mechanism/device for generating keys and creating an electronic signature/seal in its infrastructure;
- issues qualified certificates for electronic signatures/stamps after verifying the information provided by means permitted by law;
- securely stores and maintains information related to the certificates issued and the operational work of the systems;
- complies with the established operating procedures and rules for technical and physical control, in accordance with the Certificate Policy and Certification Practice Statement;
- upon request, issues the relevant types of certificates, complying with the terms and procedures in this document, the relevant Policies and generally accepted standards:
  - certification services - X.509, PKCS # 10, PKCS # 7, PKCS # 12;
  - time-stamping - recommendation RFC 3161;
  - verification of the status of a certificate - recommendation RFC 2560;
- notifies the Users of the fact of its accreditation;
- creates an opportunity for immediate suspension and revocation of a qualified certificate;
- revokes and suspends certificates under the terms and conditions of the relevant Policy;
- immediately informs the interested parties after suspension of a certificate;

- provides conditions for precise verification of the time of issuance, suspension, renewal and revocation of certificates;
- performs identification and authentication procedures for the Signature Owner/Creator of a seal;
- measures against forgery of certificates and for preserving the confidentiality of data disclosed to it in the process of creating the signature;
- uses trustworthy systems to store and manage certificates;
- ensures that only duly authorized employees have access to make changes to the data, and verify the authenticity and validity of the certificates;
- takes immediate action in case of occurrence of technical problems relating to security;
- upon expiration of the validity of the Qualified Certificate, revokes its validity;
- informs the Signature Owners/Creators of a seal and the Relying Parties of their obligations and due diligence in the use and reliance on the certification services provided by Evrotrust as well as of the proper and safe use of certificates issued and of certification services related thereto;
- uses and stores the collected personal and other information solely for the purposes of its activities on providing certification services in accordance with the national legislation;
- does not store or copy data to create user private keys;
- maintains supporting means that enable it to carry out its activities;
- takes out insurance for the time of its activity;
- maintains trusted personnel with the necessary expertise, experience and qualification to perform the activity;
- maintains a certificates register in which publishes the issued qualified certificates
- maintains a web site on which an up to date Certificate Revocation List (CRL) is published, other circumstances and electronic documents pursuant to this document and the national legislation;
- provides access without restrictions to the certificates register;
- provides protection against any unauthorized changes to the maintained certificates register, as a result of unregulated and unauthorized access or by accident;
- immediately publishes the issued certificates in the certificates register;
- creates conditions for each Relying Party to check the status of a issued and published certificate in the certificates register;

- performs periodic internal audits of the activity of the Certification Authority and the Registration Authority;
- performs external audits by independent auditors and publishes the results of the audit on its site;
- uses certified software and hardware in its business as well as secure and reliable technology systems;
- maintains on the Evrotrust website a list of Registration Authorities, a list of recommended software and hardware to be used by the users, blanks, forms, standard contract template, etc. documents for the benefit of the users;
- when providing services that do not require a secure cryptographic device, Evrotrust applies all obligations specified for NCP in ETSI EN 319 411-1;
- when providing services that require a secure cryptographic device, Evrotrust applies all obligations specified for NCP + in ETSI EN 319 411-1;
- when providing certificates in accordance with QCP-n-qscd and QCP-l-qscd policies, Evrotrust applies all obligations specified for NCP + in ETSI EN 319 411-1;
- when issuing a certificate to a legal entity in accordance with policy QCP-w Evrotrust applies all obligations specified for EVCP in ETSI EN 319 411-1;
- when issuing a certificate to a natural person in accordance with the QCP-w policy, the Evrotrust applies all the obligations specified for the NCP in ETSI EN 319 411-1;
- Evrotrust generates and manages users' private keys in a way that the secret and integrity of the keys is not compromised;
- In cases where Evrotrust has information that the private key of a user has been provided to an unauthorized person or Organisation that is not affiliated to the holder/creator, Evrotrust shall revoke all certificates that include the public key corresponding to messages compromised private key;
- Evrotrust shall not keep copies of the holder's/creator's private key.

The Provider shall be responsible before the Signature Owner for any damages caused by gross negligence or intent:

- as a result of a failure to meet the requirements of Regulation (EC) No 910/2014 in the performance of its activity on providing qualified certification services;
- as a result of false or missing data in the Qualified Certificate at the time of its issue;

- as a result of damages caused in the event that at the time of the issuance of the certificate the person named as Signature Owner/Creator of a seal did not have the private key corresponding to the public key;
- as a result of the algorithmic discrepancy between the private key and the public key entered in the certificate.
- as a result of non-compliance with its obligations to issue and manage qualified certificates;
- as a result of entering false or missing data in the certificates;
- as a result of any omissions in establishing the identity of the Signature Owner/Creator of a seal.

With a view to PSD2 compliance, if a NCA requests information related to issued certificates containing a payment institution licence number of a Payment service provider (PSP) registered with the same NCA, it is the responsibility of Evrotrust to provide that information, which is offered for consideration. Once the due payment is made, Evrotrust feeds to the NCA information on the issued certificates and specifies their number, type, serial number and validity period.

In the event that, before the end of validity of an issued certificate, the status of the qualified electronic signature/seal creation device (QSCD/smart card) on which it is recorded is changed in a way affecting the validity of the certificate, Evrotrust shall take actions in accordance with ETSI EN 319 411-2 requirements for terminating all active certificates affected by the change. Individuals whose certificates are affected will be promptly notified of the termination by email sent to the email address listed in the certificate or provided for contact. In these cases, the costs of reissuing or renewing the certificate and replacing the device with one whose status allows its use for the secure creation of a qualified electronic signature/seal are at the customer's expense.

9.6.2 LIABILITIES, RESPONSIBILITY AND GUARANTEES OF THE REGISTRATION AUTHORITY

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

Evrotrust is responsible for the actions of the Registration Authority in the Evrotrust infrastructure.

Evrotrust guarantees that the Registration Authority:

- performs its business while using reliable and secure devices and software;
- provides services that are in accordance with national legislation and does not infringe the copyrights and licensed rights of the users;
- makes the necessary efforts to perform proper user identification, correctly and accurately inputs the data in the Evrotrust database and updates this information at the time of confirmation of the data;
- does not make any deliberate errors or does not insert inaccuracies in the information contained in the certificates;
- its services are in accordance with the generally accepted standards: X.509, PKCS # 10, PKCS # 7, PKCS # 12;
- its services are provided on the basis of procedures that comply with the recommendations of "Certification Practice Statement"; This applies to:
    - user authentication procedures,
    - verification procedures to prove a private key associated with a public key;
    - procedures for accepting, processing and confirming or rejecting users' requests for issuance, renewal, suspension and revocation of certificates;
    - procedures for requesting confirmation from a Certification Authority based on already accepted user request for the issuance, renewal, suspension or revocation of a certificate;
    - procedures for creating an archive of the applications collected and data received from the users;
    - procedures for generating user keys;
    - procedures for personalization and issuance of electronic cryptographic cards on which the certificates and the key pair are stored;
    - participate in external and internal audits of Evrotrust.

The Registration Authority undertakes to:

- present to Evrotrust recommendations, especially those resulting from the audits;
- to ensure protection of personal data in accordance with the Law for Personal Data Protection, GDPR and the relevant legislation;
- to keep the private keys of the operators in safe custody in accordance with the security requirements specified in this document;

- not to use personal operator keys for purposes other than those specified in this document.

9.6.3 OBLIGATIONS OF THE USERS

The Signature Owner/Author of a seal, or the person duly authorized by the Author of a seal, identified in the Qualified Certificate, has the following obligations:

- to become acquainted with and to comply with the terms of the Contract, the Certificate Policy and Certification Practice Statement of Evrotrust, as well as the requirements in the other documents published in the web site of Evrotrust;
- when submitting requests for issuance and management of certificates to provide true, accurate and complete information that Evrotrust requires under the Contract, the legal requirements, the applicable Policies and Practices;
- to generate cryptographic keys by using a secure method and algorithm in accordance with the requirements of Regulation (EU) No 910/2014 and to use approved by Evrotrust electronic signature creation device/electronic stamp creation device;
- to verify the completeness and the accuracy of the content of the authentication information provided by it in the DN (Distinguished Name) field of the issued certificates. In the event of a discrepancy between the submitted information and the certified content, the user must immediately notify Evrotrust;
- to discontinue the use of the certificate in case of doubt about loss or compromise of the private key and to file with Evrotrust an application for its suspension;
- to discontinue the use of the certificate in the presence of obsolete, altered, incorrect and/or false information included in the issued certificate and to file a request for suspension of the certificate;
- before using the new certificate, to change the current PIN to access the electronic signature/stamp creation device where the private key is stored;
- to apply due diligence and to take the necessary measures to prevent the private key from compromising, loss, disclosure, modification or other unauthorized action;
- to use the certificate issued by Evrotrust for lawful purposes only and in accordance with the policy and practice specified therein;
- to approve the terms and conditions set out in the Contract between him/her and Evrotrust; This approval must be done with a handwritten signature on the Contract;

- to approve the certificate issued to him/her;
- not to disclose the access password for the electronic signature/stamp creation device to unauthorized persons;
- not to make their private key available to others.

9.6.4 DUE CARE OF RELIABLE PARTY

Persons who rely on a qualified electronic signature/seal certificate shall have basic knowledge of the principles of use and applicability of the electronic signature/seal and the services related to the use of a qualified electronic signature/seal certificate.

The relying party should take due care, by:

- trusting certificates only in terms of the Policy on their purpose and the limitations and conditions under which they were issued;
- verifying the status of the certificate in the certificates register maintained by Evrotrust. Verification of the electronic authenticity and integrity of the certificate outside the certificates register or in an outdated Certificate Revocation List (CRL) does not provide for verification of its validity and all damages incurred as a result of actions taken, after making only such an inspection, shall be at the expense of the Relying Party;
- verifying the validity of the electronic signature/seal of electronically signed statements, as well as the validity of the electronic signature of Evrotrust along the chain of certificates to the basic certificate;
- ensuring that the applications with which the certificate is used, are functionally applicable to the intended purpose, for which it is issued, as well as in view of the level of security specified in the relevant Policy;
- to verify that the signature/seal, accompanied by the certificate, has not been used for purposes and for value of transactions beyond the limits and purposes entered in the certificate;
- to make sure that the length of the keys used meets the security requirements of the Relying Party;
- to make sure that the certificate was valid at the time of creation of the electronic signature/seal.

Due diligence of the Relying Party is to use a mechanism for secure verification of electronic signature/seal that ensures that:

- the public key used to verify the signature/seal matches the one presented to it;
- the verification of the use of the private key is securely confirmed and the results of this verification are fairly presented;
- if necessary, the content of the signed electronic document could be determined;
- the authenticity and validity of the certificate at the time of signing are reliably verified;
- the results of the verification and the electronic identity of the Signature Owner/Creator of a seal are correctly presented;
- any changes relevant to security are identifiable.

The verification of the intended purpose of the certificate shall be carried out on the following data contained in the certificate profile:

- Policy according to which an electronic signature/seal certificate is issued and managed, specified in the "Certificate Policies" field;
- The intended purpose and the limitations of the validity of the certificate, described in the "Key Usage" and "ExtendedKey Usage" fields;
- Signature Owner/Creator of a seal details, specified in the "Subject" field.

Evrotrust shall not be held liable for any damages incurred to the Relying Party resulting from failure to perform due diligence. Any document with a defective or questionable electronic signature/seal should be rejected or possibly subjected to other procedures that make it possible to indicate its validity. Any person who approves such a document shall be responsible for any consequences.

9.6.5 OBLIGATIONS OF OTHER PARTIES

9.6.5.1 OBLIGATIONS OF THE QUALIFIED TIME-SPAMPING AUTHORITY

The Qualified Time-Stamping Authority issues qualified time-stamping certificates in accordance with the requirements laid down in Regulation (EU) No 910/2014, standards and standardization documents, technical and organizational conditions in Evrotrust ensuring secure and reliable conditions for creation and verification of electronic time-stamps, Certification Qualified Certificate Policies. The issuance is done using "Evrotrust Timestamp TSU 2024" signing unit.

Evrotrust guarantees that:

- uses security technologies, operating procedures and security management procedures to prevent any possibility of manipulating the time;

- ➢ uses cryptographic algorithm parameters in accordance with Regulation (EU) No 910/2014;
- ➢ provides technical and organizational conditions for the implementation of the required Policies for the issuance of a qualified electronic Time-stamp Tokens certificate and technical conditions for the devices for creation and verification of electronic time-stamps;
- ➢ defines at least one hash function that can be used to create time stamped hash data;
- ➢ uses universal time coordinated – UTC with the maximum allowable delay between the time of receipt of the request and the issuance of the time-stamping certificate for the time of 1 (one) second.

Evrotrust guarantees that:

- ➢ Provides non-stop access (24/7/365) of support services, excluding technical maintenance time, with the accessibility and accuracy being guaranteed, even if several users are simultaneously connected to the application;
- ➢ based its business on reliable devices and software in accordance with the requirements set forth in: CAW 14167-1 Security Requirements for Trustworthy Systems, Managing Certificates for Electronic Signatures - Part 1: System Security Requirements and ETSI TS 102 023 Policy requirements for time-stamping authorities;
- ➢ carries out its activities and services in accordance with the applicable legislation;
- ➢ issues Time-stamp Tokens in accordance with ETSI EN 319 422 Time-stamping protocol and time-stamp profiles.

9.6.5.2 OBLIGATIONS OF THE QUALIFIED CERTIFICATION AUTHORITY FOR VALIDATION

The qualified validation authorities of Evrotrust performs their functions in accordance with the requirements set out in Regulation (EU) No 910/2014. The requirements determine the technical and organizational conditions in the Evrotrust operation, the policies for certifying a qualified certificate, the technical requirements for the Signature/Stamp Creation/Verification Devices, electronic time-stamping certificates and electronic certificates for websites authentication.

Evrotrust guarantees that:

- ➢ uses operational and security management procedures that exclude any possibility of manipulating the status of the certificates or the data;

- verifies the validity of electronic signatures/stamps, electronic time-stamping certificates and electronic certificates for websites authentication, used in accordance with the requirements of Regulation (EU) No 910/2014;
- Qualified validation authorities check the status of the certificates in accordance with the RFC 2560 Online Certificate Status Protocol (OCSP) recommendation.

9.6.5.3 OBLIGATIONS OF THE QUALIFIED OPERATIONAL CERTIFICATION AUTHORITY FOR QUALIFIED ELECTRONIC SIGNATURES/STAMPS

The obligations of the Qualified Operational Certification Authority for qualified electronic signatures/stamps of Evrotrust "Evrotrust RSA Operational CA", carries out its functions in accordance with the requirements laid down in Regulation (EU) No 910/2014 for determining the technical and organizational conditions in the activities of the suppliers. The requirements relate to the Qualified Certification Policies and the technical requirements for Signature/Stamp Creation/Verification Devices.

Evrotrust uses operational and security management procedures that preclude any possibility of manipulating the status of the certificates or the data.

9.6.5.4 OBLIGATIONS OF EVROTRUST REGARDING THE CERTIFICATES REGISTER AND WEB SITE OF THE PROVIDER

The certificates register and web site of the provider are managed and controlled by Evrotrust, as it guarantees that:

- publishes and archives qualified certificates of the qualified root certification authority "Evrotrust RSA Root CA", qualified validation authority "Evrotrust RSA Validation", qualified time stamp authority "Evrotrust TSA", qualified operational certification authority "Evrotrust RSA Operational CA", qualified validation authority "Evrotrust RSA QS Validation", qualified operational certification authority "Evrotrust Services CA", qualified validation authority "Evrotrust Services Validation" and other certificates of the provider;
- publishes and archives the Certificate Policy and Certification Practice Statement, contracts with the clients, lists of recommended applications and devices, and a list of Registration Authorities, as well as other documents related to its activities;
- provides access to qualified certificates, except in cases when the Signatory has not

expressed consent and only in respect to his certificate;

- gives access to certificate status information by publishing a Certificate Revocation List (CRL), or by Online Certificate Status Protocol (OCSP);
- provides non-stop access to the information in the certificates register of the provider for a Certification Authority, Registration Authority, clients and relying parties;
- publishes a Certificate Revocation List (CRL) without delay and in accordance with the deadlines specified in this document.

9.7 WAIVER OF LIABILITY

The liability of Evrotrust is based on the general rules set out in this Certification Practice Statement and is in accordance with the necessary legal acts in force in the Republic of Bulgaria. Disclaimers should be defined in contracts between the users and Evrotrust.

EVROTRAST shall not be held liable in cases where the damages incurred are as a result of failure to exercise due diligence, failure to fulfil obligations, or lack of knowledge of the field of the PKI technology ("Public Key Infrastructure") by the Signature Owners or the Relying Parties.

Evrotrust shall not be held liable also in cases of any damages caused by:

- the use of a certificate outside the scope of the intended purposes and limitations of its operation stated in it in relation to the purposes of use and limitations on the value of the transactions;
- unlawful actions by Signature Owners or the Relying Parties;
- providing the way of identifying the signature/seal creation device and access to the private key by the Signature Owner/Creator of a seal to third parties;
- incidental events of the nature of force majeure, including malicious actions of third parties (hacking attacks, deprivation of the signature/seal creation device, access to the private key, becoming aware without the Signature Owner's knowledge of the way of identification, etc.)
- use of a certificate not issued, or used in accordance with the requirements and procedures of Practice and Policy of Evrotrust;
- use of an invalid certificate (certificate that has been suspended or revoked);
- not timely action to revoke or suspend a certificate (due to a delay of request by the Signature Owner/Creator of a seal, or for reasons beyond the control of Evrotrust);
- a compromised private key, corresponding to the public key in the certificate at fault

of the the Signature Owner/Creator of a seal;

- poor quality and functionality of the software products and hardware devices used by the Signature Owner/Creator of a seal and the Relying Parties.

Evrotrust is not responsible for the attachment contents. All the risks that may occur when downloading the attachments are responsibility of the users who exchange them.

9.8 LIMITATIONS OF LIABILITY

For Qualified Electronic Signature/Seal certificates issued, the Provider is responsible within the limits of the transaction value limits entered in the certificates.

9.9 RESPONSIBILITY OF THE SIGNATURE OWNER/CREATOR OF A SEAL

Signature Owner/Creator of a seal shall be held liable before Evrotrust and all relying persons, if:

- in creating the private-public key pair he/she has used an algorithm and electronic signature/seal creation devices that do not meet the requirements of Regulation (EU) No 910/2014;
- does not exactly meet the security requirements determined by Evrotrust;
- does not request that Evrotrust suspends or revokes the certificate after he/she has become aware that the private key was used improperly or is in danger of unauthorized use;
- has made untrue statements to Evrotrust that are also related to the content or the issuance of the qualified certificate;
- when the certificate is issued with a registered Creator of a seal and a person authorized by him/her, he/she is responsible for the failure of the authorized person to fulfill his/her obligations.

Subscriber, Signatory/Creator or the representative of the legal entity is responsible for the content of the attachments and the consequences of their use.

9.9.1 RESPONSIBILITY OF THE SIGNATURE OWNER/CREATOR OF A SEAL TO EVROTRUST

Signature Owner/Creator of a seal shall be held liable to Evrotrust if he/she or the person authorized by him/her has provided untrue data, respectively, has withheld data relevant to the content or issuance of the certificate, as well as when he/she did not properly store the private key corresponding to the public key specified in the certificate.

9.10 TERM AND TERMINATION OF THE "CERTIFICATION PRACTICE STATEMENT"

9.10.1 TERMS

This Practice shall come into force upon its approval by the Board of Directors of Evrotrust and its publication on the Evrotrust web site. Appendices to this document shall come into force after their publication on the Evrotrust web site.

The provisions in this document shall be valid until the next version of "Certification Practice Statement for Qualified Certification Services" is issued and published in the repository on the Evrotrust website.

9.10.2 TERMINATION

Upon termination of the operation of Evrotrust, the validity of the Practice, as well as the provisions contained in this document shall be terminated.

Provider shall keep duly and securely all previous versions/revisions of this document.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of the Certification Services Contract, Signature Owner/Creator of a seal and the Relying Parties shall remain bound by this document from the point of view of the issued User Qualified Certificates for the remainder of the period of validity of these certificates.

9.11 NOTIFICATION AND COMMUNICATION BETWEEN THE PARTIES

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

The choice of means can be done depending on the type of information and the way of use of the services of Evrotrust.

Information on any breakthrough in the security of the private keys of the Certification Authorities should be posted on the Evrotrust web site, making it available to all stakeholders.

9.12 AMENDMENTS TO "CERTIFICATION PRACTICE STATEMENT"

Amendments to the Practice may result from observed errors, updates and suggestions from affected parties. In the event of an invalid clause in this document, the validity of the entire document is retained and the contract with the Signature Owner/Creator of a seal is not violated. The invalid clause is replaced by a lawful norm.

Evrotrust may make revision changes to this document that do not affect the content of the rights and obligations contained therein.

Changes that lead to a new version/revision of the document shall be published on the Evrotrust website.

9.13 DISPUTE RESOLUTION

Evrotrust has a procedure for filing, examining and resolving suggestions, complaints, signals and claims received by users, clients or relying parties regarding the provision of services or other related issues.

Only discrepancies or disagreements between persons who are parties to the contract with Evrotrust may be subjects of disputes. Disputes or claims regarding the use of certificates and trust services provided by Evrotrust will be resolved through mediation based on information submitted in writing. Every claim must contain a description of the subject, cause or circumstances related to the problem being addressed, as well as the full name, address, e-mail and telephone number to contact the claimant. Copies of documents related to the described subject may be attached to the submitted complaints.

When filing a complaint, the user shall indicate the subject of the complaint, his/her preferred way to satisfy the complaint, respectively the amount of the claimed amount, and contact address. When filing a complaint, the user must also attach the documents on which the claim is based. When filing the complaint of the service, the user may claim for provision of the services in accordance with the contract, a price discount or refund.

Claims, signals and complaints shall be filed as follows:

➢ Personally, in writing, on paper, and personally signed signed (by way of exception, only complaints are allowed to be made orally) in the office at the following address:

Evrotrust Technologies AD
Sofia, 1766
Okolovrasten pat" 251G, Business center MM, floor 5
telephone, Fax: + 359 2 448 58 58
email: office@evrotrust.com

➢ At the e-mail address of Evrotrust (office@evrotrust.com or dpo@evrotrust.com;), signed with a qualified electronic signature.

Evrotrust considers every claim or complaint received and prepares a written response with proposals for action to be taken (if applicable) within 7 days. When the decision of a specific claim or complaint requires the collection of additional information on the case, which requires more time, the claimant/complainant shall be notified in writing where the relevant reasons shall be specified. Evrotrust reviews a received claim or complaint and sends a final response to the claimant/complainant within 1 (one) month.

9.14 APPLICABLE LAW

For all matters not settled in this document the provisions of the Bulgarian legislation shall apply.

9.15 COMPLIANCE WITH THE APPLICABLE LAW

Evrotrust applies the following requirements to ensure that it operates legally and reliably:

➢ Evrotrust provides users and all stakesignatorys with policies, practices, certificates and declarations for successfully performed inspections to prove how it meets the applicable legal requirements;

➢ Evrotrust provides trust services and products to end users - people with disabilities, where possible;

➢ Evrotrust provides trust services taking into consideration ETSI EN 301 549 relevant to the accessibility-related needs of ICT users in the products and services;

➢ Evrotrust guarantees that it has taken appropriate technical and organisational measures against unauthorised access to the information system, illegal processing of personal data or against accidental loss, destruction or damage of personal data. Evrotrust processes personal data in accordance with Regulation (EU) 2016/679. In this respect, the provision of an online service and the authentication of online data relates only to the processing of those identification data that are adequate, appropriate and not excessive in order to provide access to that service online.

9.16 OTHER PROVISIONS

The practice does not specify any other provisions.

10. USED TERMS AND ABBREVIATIONS

10.1 APPENDIX 1: TERMS AND ABBREVIATIONS IN BULGARIAN

Validation	Validation means the process of verifying and confirming that an electronic signature or a seal is valid
Validation data	Validation data means data that is used to validate an electronic signature or an electronic seal
Person identification data	Person identification data means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established
Electronic signature creation data	Electronic signature creation data means unique data which is used by the signatory to create an electronic signature
Relying party	Relying party ("Relying Parties") means a natural or legal person that relies upon an electronic identification or a trust service
Qualified trust service provider	Qualified trust service provider means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body
PIN	Personal Identification Number (of a citizen)
Electronic time-stamp	Electronic time-stamp means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time
Electronic document	Electronic document means any content stored in electronic form, in particular text or sound, visual or audio-visual recording
Electronic seal	Electronic seal means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity The electronic seal serves as evidence that an electronic document is issued by a legal entity and guarantees the reliable origin and integrity of the document. Except for the verification of the authenticity of a document issued by a legal entity, electronic stamps can be used for the verification of the authenticity the digital assets of a legal entity such as a software code or servers

Electronic signature	Electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
Electronic identification	Electronic identification is the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
TSU	Timestamping Services Unit
Qualified electronic time-stamp	Qualified electronic time-stamp means an electronic time-stamp which meets the requirements: a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably b) it is based on an accurate time source linked to Coordinated Universal Time; and c) it is signed using an advanced electronic signature or an advanced electronic seal of the qualified trust service provider, or by some equivalent method
Qualified electronic seal	Qualified electronic seal means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.
Qualified electronic signature	Qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
Qualified certificate for website authentication	Qualified certificate for website authentication means a certificate for website authentication, which is issued by a qualified trust service provider
Qualified certificate for electronic signature	Qualified certificate for electronic signature means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements according to the normative framework
CRC	Communications Regulation Commission
MRS	Materially responsible person

PIN	Personal Identification Number
Practice	Practice in the provision of certification services (Certification Practice Statement) is a document containing rules on the issuance, suspension, renewal and termination of certificates, the conditions for certificates access.
Policy	Policy for the provision of certification services (Certificate Policy) is a document describing the policy which the provider follows when issuing certificates, as well as for all services provided
Registration Authority	Registration Authority ("RA") is a separate structure of a Provider which carries out some of the activities or all of the following related to: accepting, checking, approving or rejecting requests and electronic applications for issuance and management of certificates, registering the submitted requests to the Certification Authority for issuing and making changes to the status of certificates, performing the respective identity authentication checks, respectively the identity of the Signature Owners, as well as specific data about them, with the lawful means and in accordance with the Certificate Policy and Certification Practice Statement.
Regulation (EU) № 910/2014	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic identification and Trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
Electronic identification means	Electronic identification means means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service
Electronic identification scheme	Electronic identification scheme means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons
Author of a seal	Creator of a seal means a legal person who creates an electronic seal
Signature Owner	Signature Owner means a natural person who creates an electronic signature
Authentication	Authentication means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed
Time-Stamping	Data in electronic form linking other electronic data to a certain point in time,

certificate	providing evidence that these data exist at that time
Certificate for electronic seal	It is issued to legal entities and serves to validate integrity and original of data/documents.
Certificate for electronic signature	Certificate for electronic signature means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person
Trust service	Trust services means electronic services normally provided for remuneration by the Trust Services Provider which consists of: the creation, verification, and validation of electronic signatures, electronic seals or electronic time-stamps, electronic registered delivery services and certificates related to those services, or the creation, verification and validation of certificates for website authentication; or the preservation of electronic signatures, seals or certificates related to those services
Certification service for website authentication	Certification service for website authentication provides means by which a visitor to a website can be confident that behind the website there is a real and legitimate subject
Certification Authority	Certification Authority "CA" is a distinct structure of a Provider that carries out the activities on providing certification services. The Certification Authority has no separate legal personality and all actions and acts performed by its employees are performed in their capacity of employees of Evrotrust within the limits of their powers
Electronic seal creation device	Electronic seal creation device means configured software or hardware used to create an electronic seal
Qualified electronic seal creation device	Qualified electronic seal creation device means an electronic seal creation device that meets the requirements in Regulation (EU) № 910/2014
Qualified electronic signature creation device	Qualified electronic signature creation device means an electronic signature creation device that meets the requirements in Regulation (EU) № 910/2014
Electronic signature creation device	Electronic signature creation device means configured software or hardware used to create an electronic signature

Advanced electronic seal	advanced electronic seal means an electronic seal, which meets the requirements: a) it is uniquely linked to the creator of the seal b) it is capable of identifying the creator of the seal c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable
Advanced electronic signature	Advanced electronic signature means an electronic signature which meets the requirements: - it is uniquely linked to the signatory; - it is capable of identifying the signatory; - it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and - it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable
Legal persons	Legal persons within the meaning of the Treaty on the Functioning of the European Union (TFEU) mean all entities constituted or regulated under the law of a Member State, whatever their legal form

10.2 APPENDIX 2: TERMS AND ABBREVIATIONS IN ENGLISH

ASN.1	Abstract Syntax Notation One
A	Actuality
BG	Bulgaria
C	Country
CA	Certification Authority
CC	Common Criteria
CN	Common Name
CP	Certificate Policy
CSP	Cryptograph Services Provider

CPS	Certification Practice Statement
CRL	Certificate Revocation List
DSA	Digital Signature Algorithm
DN	Distinguished Name
E	E-mail
e-ID	Electronic Identity
Extended key usage	X.509 Certificate extended key usage
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
ISO	International Standardization Organization
Issuer	X.509 Certificate Issuer
IP	Internet Protocol
L	Location
N	Number
NCA, National Competent Authority	National Competent Authority
OU	Organization Unit
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSD2, Payment Services Directive 2	The revised Payment Service Directive: DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
PSP, Payment Service Provider	Payment Service Provider
RA	Registration Authority
RSA	Rivest-Shamir-Adelman
SSCD	Secure Signature Creation Device

SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
S	Street
T	Title
Token	Cryptographic token
URL	Uniform Resource Locator

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.

[i] *If there are no included attributes for **organizationName** and **organizationIdentifier** the attribute **id-etsi-qcs-SemanticsId-Legal** is also not included.*

[ii] *If the attribute **id-etsi-qcs-QcLimitValue** is included in the certificate it specifies the limitation on the value of transaction for which this certificate can be used to.*

[iii] In accordance with the requirements of ETSI TS 119 412-2, the "Key Usage" extension must be of type "A" only, i.e. must contain only the value "Non-repudiation". Due to the context of applicability of certificates in the Republic of Bulgaria and other European countries, Evrotrust allows the use of type "F" (values: "Non-repudiation", "Digital Signature", "Key Encipherment") in the "Key Usage" extension in the cases , when certificates are used in a role as a means of establishing an encrypted TLS connection and encrypting data.