POLICY

FOR QUALIFIED CERTIFICATION SERVICES

FOR ADVANCED ELECTRONIC SIGNATURE / SEAL

CONTENTS

1 INTRODUCTION

"Policy for qualified certification for advanced electronic signature/seal" (Policy/CP/Certificate Policy) is a document describing the general rules and regulations applied by "Evrotrust Technologies" AD (Evrotrust) in the creation and management of qualified certificates for advanced electronic signatures/seals, the types of qualified certification services applicable for those certificates, as well as their scope of application.

Upon issuance of qualified certificate for advanced electronic signature/seal from Evrotrust, procedures are in place to ensure a high level of reliability and security of the authenticated information identifying the Users. Procedures are in place to ensure reliability and security when issuing, publishing and managing (stopping, resuming, terminating and renewing) qualified certificates, signing/printing, storing a private key and using it in a variety of applications.

Introduction to the objectives and role of the "Policy for qualified certification for advanced electronic signature/seal" is particularly important for Users (Signatories/Creators) and Relying Parties in terms of the feasibility of these services.

The relationship between Evrotrust and the end-user are governed by the General Terms and Conditions of the Contract for Trust, Information, Cryptographic and Other Services, or, where applicable, by a contract for provision of the respective service, the General Terms being an inseparable part thereof.

The prices of certificates and services for issuing and managing qualified certificates are contained in the Evrotrust Tariff, available on the Evrotrust web site.

1.1 REVIEW

The "Policy for qualified certification for advanced electronic signature/seal" document refers to qualified certificates issued by Evrotrust pursuant to Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Regulation (EU) No 910/2014) and in accordance with the applicable legislation in the Republic of Bulgaria.

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

The policy complies with the following documents:

- ETSI EN 319 411-2 „Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates";
- ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers";
- 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 319 412-5: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements";
- ETSI TS 101 456: „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates";
- ETSI TS 119 461 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects";
- ETSI TS 119 495: „Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366";
- 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

The issue of Qualified Certificates for Advanced Electronic Signatures/Seals is associated with:

- issuance of a qualified certificate to a natural person (Signatory) – has the character of a Qualified Certificate for Advanced Electronic Signature;
- advanced electronic seal of a legal entity (Creator of a seal) – Has the character of a Qualified Certificate for Advanced Electronic Seal.

"Policy for qualified certification for advanced electronic signature/seal" to Evrotrust Technologies AD is a public document. It may be amended at any time by Evrotrust and any new revision shall be notified to the interested parties by publishing on the Evrotrust website: https://www.evrotrust.com.

1.2 NAME AND IDENTIFIER THE POLICY

This document is entitled "Policy for Qualified certification for Advanced Electronic Signature/Seal" by Evrotrust Technologies AD.

The certificates contain a policy identifier that can be used by the Relying parties to determine their applicability to an application as described in IETF RFC 3647 recommendation, section 3.3.

The policy identifiers of Qualified Certificates specified in this document are:

QCP-n:

Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)

policy-identifiers(1) qcp-natural (0)

QCP-l:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112)

policy-identifiers(1) qcp-legal (1)

The Provider supports and applies a Qualified Certification Policy based on the rules defined in ETSI EN 319 411-1 with Object Identifier (OID) as follows:

Certificate type	Object Identifier
Evrotrust Qualified Natural Person Certificate for AES QCP-n	1.3.6.1.4.1.47272.2.7 *(relevant to policy with O.I.D. = 0.4.0.194112.1.0)*
Evrotrust Qualified Legal Person Certificate for AESeal QCP-l	1.3.6.1.4.1.47272.2.8 *(relevant to policy with O.I.D. = 0.4.0.194112.1.1)*
Evrotrust Qualified PSD2 Legal Person Certificate for AESeal	1.3.6.1.4.1.47272.2.8.1 *(relevant to policy with O.I.D. =*

QCP-l	*0.4.0.194112.1.1)*

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

1.3 PARTICIPANTS IN THE INFRASTRUCTURE

Evrotrust, as a qualified provider of qualified certification services, provides generation and management services (suspension, resumption and termination) of Qualified Certificates through the Authentication Body "Evrotrust RSA Operational CA" and Services for Identity and Authentication of Users through the Registration Authority. Other participants in the Evrotrust infrastructure are Users and Relying Parties.

1.3.1 CERTIFYING AUTHORITY

"Evrotrust RSA Operational CA" is a certifying authority that issues qualified certificates for advanced electronic signatures/seals that are managed under this policy.

1.3.2 REGISTERING AUTHORITY

The registration authority is a separate structure of Evrotrust but may also be an external legal entity to which Evrotrust assigns services of registration, identification and authentication of Evrotrust users.

The Registration authority performs the following activities:

- ➢ accepts requests for qualified certificates, approves or rejects these requests in accordance with Evrotrust's internal rules of approval;
- ➢ verifies the identity of the persons applying for certificates;
- ➢ verifies that the issued certificate is handed to the User (Signatory/Creator);
- ➢ terminates qualified certificates on the basis of the Evrotrust termination rules.

Contact details of the Evrotrust Registration Authority are available on the Evrotrust web site.

1.3.3 USERS

Any natural person or legal enity who has a written contract with Evrotrust is a user of a qualified certification service provided by Evrotrust.

Users are:

- natural person (Signatory) who creates an advanced electronic signature;
- natural person (Signatory) who is the authorized representative of a legal entity and creates an advanced electronic signature;
- legal entity (Creator of a seal), which creates an advanced electronic seal.

Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

1.3.4 RELYING PARTIES

Relying Party is a natural or legal person accepting a qualified certificate issued by the Evrotrust infrastructure after having verified the advanced electronic signature/seal of a User of Qualified Certification Services to the Provider.

1.3.5 OTHER PARTICIPANTS

Evrotrust reserves the right, if necessary, to conclude contracts with outside persons for the provision of certain certification services.

1.4 USE AND APPLICABILITY OF QUALIFIED CERTIFICATES

1.4.1 APPLICABILITY OF QUALIFIED CERTIFICATES

Qualified Certificate of natural person (Signatory)/Legal Entity (Creator) or authorized representative of a legal entity named as Signatory in the certificate may be used to create an advanced electronic signature/seal in electronic documents and attachments/transactions that require high level of information security.

1.4.2 PROHIBITION OF USE OF QUALIFIED CERTIFICATES

Qualified Evrotrust certificates should not be used in a manner inconsistent with their stated purpose and scope/Policy.

Qualified certificates issued in accordance with this Policy must not be used for unlawful purposes.

1.5 POLICY MANAGEMENT

1.5.1 POLICY MANAGEMENT ORGANIZATION

Evrotrust is responsible for the management of this Policy.

Each version of the Policy is in force until the approval and publication of a new version. Each new version is developed by Evrotrust employees and is published after approval by the Evrotrust Board of Directors.

Users are required to comply only with the valid version of the Policy at the time of use of Evrotrust services.

1.5.2 CONTACT PERSON

The contact person for the document "Policy for the award of a qualified certificate for advanced electronic signature/seal" 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

1.5.3 RELATIONSHIP BETWEEN POLICY AND PRACTICE

The "Policy for qualified certification for advanced electronic signature/seal" (CP/Policy) and the "Practice for providing qualified certifying services" (CPS/Practice) cover the same set of topics which serve the Users and the interests of the Relying Parties, so as to allow them to rely on the secure and reliable application of qualified certificates for advanced electronic signature/seal issued by Evrotrust.

The main difference between both documents is the focus of their provisions and their intended purpose. The policy examines the requirements and the implementation of the standards imposed by Evrotrust's created infrastructure and identifies the participants in the certification services activities. Practice, on the other hand, indicates how the Certification Authority and other infrastructure participants apply procedures and controls to meet the requirements of the Policy. In other words, the purpose of both documents is to ensure the unity of rules and procedures how the participants in the Evrotrust infrastructure perform their duties and responsibilities.

The main difference between Policy and Practice is that with a Practice Certification Authority can support several Policies used for different applications or with different scope for different Relying Parties.

1.5.4 CONTACT PERSON AND PRACTICE APPROVAL PROCEDURES

The person who takes decisions on the performance of the "Practice for Providing Qualified Certification Services" (CPS) and is responsible for its management is the Executive Director of Evrotrust Technologies AD.

"Practice for Providing Qualified Certification Services" (CPS) has been developed by the Evrotrust team and has been approved by the Board of Directors of Evrotrust.

Each version of "Practice for Providing Qualified Certification Services" is in effect until the approval and publication of a new version.

1.6 DEFINITIONS AND ABBREVIATIONS

1.6.1 DEFINITIONS

Certification – A certification services provider may be granted a "qualified" status for a specified period in accordance with Regulation (EU) No 910/2014 after passing a successful audit of compliance by accredited auditors;

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

Validation - The process of verifying and confirming that an electronic signature or a seal is valid.

Person identification data - A set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

Data for the creation of an electronic signature - Unique data which is used by the

Signatory to create an electronic signature;

Relying Parties – Natural persons or legal entities who are the addressees of electronic statements or other information sites and trust the certification services of Evrotrust;

Qualified trust service provider - A trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body;

Electronic time stamp - 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 and is issued in accordance with Regulation (EU) No. 910/2014;

Electronic seal - Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity; The electronic seal should serve as evidence that an electronic document was issued by a legal entity, ensuring certainty of the document's origin and integrity.

Electronic signature - Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the Signatory to sign;

Qualified trust service - A trust service that meets the applicable requirements laid down in Regulation (EU) No. 910/2014;

Qualified certificate for electronic signature - A certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Regulation (EU) No. 910/2014;

Qualified electronic time stamp - An electronic time stamp which meets the requirements laid down in Regulation (EU) No. 910/2014;

Advanced electronic seal - An advanced electronic seal, which is created by an advanced electronic seal creation application/system, and that is based on a qualified certificate for electronic stamp;

Advanced electronic signature - An advanced electronic signature that is created by an advanced electronic signature creation application/system, and which is based on a qualified certificate for electronic signatures;

Coordinated Universal Time (UTC) – Time to which the time is calculated in different time zones. It uses the International Atomic Time (TAI) as a basis;

Policy Approval Authority (PAA) – Body authorized to approve, monitor, and maintain the Certification Policy;

Compliance assessment body – A body that is accredited in accordance with Regulation (EC) No. 765/2008 as competent to assess the compliance of a qualified certification service provider and the qualified certification services provided by that provider with the requirements of Regulation (EU) No. 910/2014;

Practice (CPS) - Practice in the provision of Qualified Certification Services is a document containing rules on the issuance, suspension, revocation and revocation of certificates as well as the conditions for granting access to certificates;

CRL/Certificate Revocation List – The list containing certificates that may no longer be considered valid. The CRL is digitally signed by the issuer of the certificates – the Certifying Authority;

Creator of a seal means a legal entity who creates an electronic seal;

Private key – A string of symbols that is used in an algorithm to convert information from a readable encrypted form or vice versa – encrypted in a readable form (decryption);

Public Key – One of the key pairs used in an asymmetric cryptosystem that is accessible and can be used to verify electronic signature/seal;

Signatory of an electronic signature - A natural person who creates an electronic signature;

Certification service - An electronic service which is usually provided in return for payment consisting in: the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, registered email services, as well as certificates related to those services; or the creation, verification and validation of certificates of authenticity of a website; or the storage of electronic signatures, seals or certificates related to those services;

Electronic seal certificate - Legal entity certificate by terms of Regulation (EU) No 910/2014;

Time stamp certificate - Data in electronic form linking other electronic data to a certain point in time, providing evidence that these data exist at that time;

Certificate for electronic signature - 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;

Environment for creating an advanced electronic seal – An environment for creating an advanced electronic seal is an application or system that complies with the requirements of

Regulation (EU) No 910/2014;

Environment for the creation of an advanced electronic signature – An advanced electronic signature enrichment environment is an electronic signature application or system that complies with the requirements of Regulation (EU) No 910/2014;

Electronic signature creation environment - Application or system used to create an electronic signature is a configured software or hardware used for the creation of an electronic signature;

1.6.2 ABBREVIATIONS

QCP-l – Qualified certificate policy issued to a legal entity when the private key of the associated certificate is generated in a secure environment;

QCP-n - Qualified certificate policy issued to a natural person when the private key of the associated certificate is generated in a secure environment;

NCP + – Enhanced normalized certification policy that includes additional requirements for Qualified Certificates in accordance with Regulation (EU) No. 910/2014

CA Certification Authority – Certifying Authority;

CN Common Name – Common name;

CP Certificate Policy – Policies to provide qualified certificate for advanced electronic signature/seal;

CPS Certification Practice Statement – Certification services provision practice;

CRL, Certificate Revocation List – List of suspended and terminated certificates;

PSD2 (Payment Services Directive 2) - 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;

DN, Distinguished Name – Distinct name of subject, entered in the certificate;

Enhanced key usage – Expanded key usage goals

FIPS, Federal Information Processing Standard – Federal standard for information processing;

HSM, Hardware Security Module – Hardware Cryptographic Module;

Issuer – Publisher;

LDAP, Lightweight Directory Access Protocol – Protocol for Simple Registry Access;

OID, Object Identifier – Object Identifier;

PKCS, Public Key Cryptography Standards – Cryptographic standard for public key transfer;

PKI, Public Key Infrastructure – Public Key Infrastructure – aggregate of hardware, software, staff, Evrotrust documentation for creating, using, managing and verifying issued electronic signatures/stamps;

RA, Registration Authority – Registration Authority;

RSA, Rivest-Shamir-Adelman – Type of asymmetric cryptographic algorithm for creation of an electronic signature;

SHA, Secure Hash Algorithm – A sure hash algorithm to extract a hash-identifier;

SSL, Secure Socket Layer – Secure data transmission channel;

SMIME, Secure Multipurpose Internet Mail Extensions – A secure e-mail protocol over the internet;

2 RESPONSIBILITY FOR PUBLISHING AND STORAGE

2.1 REPOSITORY

Evrotrust maintains a repository in which current and previous versions of electronic documents (including up-to-date versions of the "Qualified Certificate for Advanced Electronic Signature/Seal Certificate" and "Practice for Qualified Certification Services") 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.

All users and trustees have permanent access to all information in the repository at: https://www.evrotrust.com. Restrictions have the relying parties, but they are related to accessing only user certificates for which access to the register of user certificates is restricted.

2.2 PUBLISHED INFORMATION

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

Qualified certificates issued are stored in a Evrotrust database. Access to these certificates can be accomplished through an online protocol to verify the status of the issued OCSP (Online Certificate Status Protocol).

For online verification of registry data, it is necessary to use appropriate software (OCSP client or access through the supplier's website.

Verification of qualified certificates issued may also be made on the CRL, which is published on the Evrotrust website and updated every 3 hours.

2.3 FREQUENCY OF PUBLICATION

The documentation, including Policy and Practice in the provision of Qualified Certification Services, Agreements, Patterns, Electronic Signature/Seal Manuals, Audit Reports, etc. issued by Evrotrust, is published on the Evrotrust web site immediately upon each update.

The Operating Certificates of the Certifying Authority are published immediately upon each issue of new certificates.

An update of the Register with the issued user qualified certificates shall be made automatically and immediately after the publication of each newly issued valid certificate.

An update of the current CRL is automatically made no more than 3 (three) hours or immediately after the revocation/termination or suspension/resumption of a valid certificate.

2.4 ACCESS TO PUBLICATIONS

Evrotrust offers directory services for information stored in the repository, providing HTTP/HTTPS and OCSP-based access.

Access to repository information is not limited by Evrotrust, except upon request of the Signatory/Creator and only in respect of a validly issued Qualified Certificate.

The information published in Evrotrust's repository is permanently accessible (24/7/365), except in the event of events beyond Evrotrust's control.

3 IDENTIFICATION AND VERIFICATION OF IDENTITY

3.1 NAMES

The certificate names requirements are as stated 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.

**The procedure for checking and entering names is described in the document “Practice of Qualified Certification Services.”*

3.2 INITIAL REGISTRATION

** The procedure for initial registration is described in the document " Practice of Qualified Certification Services."*

3.2.1 CHECK FOR PRIVATE KEY OWNERSHIP

**The procedure for owning a private key is described in the document " Practice of Qualified Certification Services."*

3.2.2 CHECKING THE IDENTITY OF A LEGAL ENTITY

**The procedure for verifying the identity of a legal entity is described in the document" Practice of Qualified Certification Services."*

3.2.3 ESTABLISHING AN IDENTITY OF A NATURAL PERSON, AN AUTHORIZED REPRESENTATIVE OF A LEGAL ENTITY

** The procedure for identifying an individual, an authorized representative of a legal entity, is described in the document " Practice of Qualified Certification Services."*

3.2.4 ESTABLISHING IDENTITY OF A NATURAL PERSON

** The procedure for identifying an individual is described in the document "Practice of Qualified Certification Services ".*

3.2.5 VERIFICATION BY THE CERTIFYING AUTHORITY

Upon successful identification and verification by the Registration Authority of the conditions for the issuance or management of a qualified certificate, a representative of the Registration Authority confirms the data to the Certifying Authority. The Certifying Authority shall immediately publish the Qualified Certificate issued in the Register of issued certificates/Issued

Certificates repository or CRL.

In Evrotrust, only the operational Certifying Authority that has issued an advanced electronic signature/seal certificate may terminate this certificate.

3.3 IDENTIFICATION AND IDENTITY VERIFICATION UPON RENEWAL A QUALIFIED CERTIFICATE

**The procedure for identification and verification of identity when renewing a certificate is described in the document "Practice of Qualified Certification Services ".*

3.4 IDENTIFICATION AND IDENTITY VERIFICATION WHEN A QUALIFIED CERTIFICATE IS SUSPENDED

**The procedure is described in the document "Practice of Qualified Certification Services ".*

3.5 IDENTIFICATION AND IDENTITY VERIFICATION WHEN A QUALIFIED CERTIFICATE IS TERMINATED

When Evrotrust, through the Registration Authority or itself, ceases a qualified certificate, it shall record this in the databases it holds with qualified certificates and publish the revoked status of the certificate in due time but not later than 24 hours after the request is received. The revocation shall become effective immediately upon its publication.

Upon termination through the Evrotrust mobile application, identity verification is not performed due to the Signatory's access to the appropriate functionality.

3.6 IDENTIFICATION AND IDENTITY VERIFICATION AFTER A QUALIFIED CERTIFICATE IS TERMINATED

The policy and practice of providing qualified certification services to Evrotrust does not allow the renewal of a qualified certificate through Renewal or Re-key after termination.

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

Evrotrust, through the Registration Authority, performs initial identification and identity verification of the Signatory/Creator if he/she requests a new certificate. Such a check is not performed if the user requests the issue of a new qualified certificate from the mobile application in which there is an active account.

4 OPERATIONAL REQUIREMENTS

**Evrotrust provides operational procedures for Qualified Certification Services applicable to Qualified Electronic Signature / Seal Certificates described in the Practice for Qualified Certification Services.*

4.1 USE OF QUALIFIED CERTIFICATE AND KEY PAIR

4.1.1 BY USERS

Users must use the private keys and their respective qualified certificates:

- in accordance with their intended purpose;
- only within the period of their validity;
- when the certificate is suspended, the user should not use the private key, especially for creating an electronic signature/seal.

Responsibility for using the private key is at the Signatory.

4.1.2 FROM RELYING PARTIES

Relying parties, including operators in the Registration Authority, must use the public keys and their respective certificates:

- in accordance with their intended purpose;
- only after checking their status and checking the electronic signature of the Certification Authority that issued the certificate;
- until the validity of a key is revoked/terminated;
- when the certificate is suspended, the relying party should not accept the public key.

4.2 RENEWAL OF QUALIFIED CERTIFICATE

Renewal of a qualified certificate means replacing a valid certificate with a new one without changing the existing information in it, except for a new serial number and a new validity period.

Renewal is only performed within the validity period of a current certificate. It must be preceded by the registration of a renewal application in an appropriate form accepted and approved by an operator in the Registration Authority, verified identity and correctness of the submitted application.

Renewal of a remote certificate issued through the mobile application is not allowed.

4.3 ISSUING A QUALIFIED CERTIFICATE BY GENERATING A NEW KEY PAIR (RE-KEY)

*****

**The procedure is described in the document "Practice of Qualified Certification Services".*

4.4 CHANGE IN QUALIFIED CERTIFICATE

Changing a qualified certificate means a change in the content of the data in a previously issued and published advanced electronic signature/seal certificate. Upon changing a qualified certificate, a new pair of keys is required to be generated.

The change is treated in the same way as issuing a new qualified certificate.

4.5 SUSPENSION AND TERMINATION OF A QUALIFIED CERTIFICATE

**The procedure is described in the document "Practice of Qualified Certification Services ".*

4.5.1 CIRCUMSTANCES FOR TERMINATION OF A QUALIFIED CERTIFICATE

Evrotrust terminates a qualified certificate issued by it, subject to the following hypotheses:

- 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;
- the user decides to terminate the contract with Evrotrust;
- death or incapacity of the Signatory/Creator;
- termination of the Representative authority of the Signatory against the Creator;
- when the User does not meet the requirements of the Certification Policy;
- if the Certifying Authority ceases its activity;
- if the User owes outstanding fees for the provision of Qualified Certification Services;
- when the reliability and security of the Certification Authority private key is compromised;
- when User who is an employee of an organization terminates his or her contract of employment and does not delete a private key corresponding to the qualified certificate issued.

4.5.2 PROCEDURE FOR TERMINATION OF QUALIFIED CERTIFICATE

4.5.2.1 QUALIFIED END-USER CERTIFICATE TERMINATION PROCEDURE

**The procedure is described in the document "Practice of Qualified Certification Services ".*

4.5.3 GRACE PERIOD FOR TERMINATION OF QUALIFIED CERTIFICATE

Before suspending the validity of a validated certificate, Evrotrust, through its Registration Authority, shall suspend the certificate validity for a grace period until the reasons for the suspension have been specified.

4.5.4 ONLINE CHECK OF A CERTIFICATE STATUS

Evrotrust provides a qualified service to check the status of issued certificates in real time. This service is based on a Protocol for Online Certificate Verification of the Status (OCSP) described in RFC 2560. Using OCSP makes it possible to obtain status information for certificates without requiring verification in the CRL.

The OCSP service generates a database-based response. The OCSP response is valid for up to 7 days. To maintain the proper system performance, OCSP responses are cached for a predetermined time (typically not more than a few hours).

Verification in real-time certificate status under the OCSP protocol can be performed via Internet at the Evrotrust website: https://www.evrotrust.com.

4.5.5 CIRCUMSTANCES FOR SUSPENSION OF A QUALIFIED CERTIFICATE

Evrotrust, through its Operator Certification Authority ("Evrotrust RSA Operational CA"), suspends a valid certificate under certain conditions.

Evrotrust takes immediate action on the request to suspend a certificate.

The time during which the certificate was suspended is deemed invalid and all electronic signatures/stamps checked with this certificate are null and void.

4.5.6 PROCEDURE FOR SUSPENDING AND RESUMING A QUALIFIED CERTIFICATE

**The procedure is described in the document "Practice of Qualified Certification Services".*

4.5.7 GRACE PERIOD OF SUSPENSION OF A QUALIFIED CERTIFICATE

Evrotrust suspends a Qualified Electronic Signature/Seal Certificate for a grace period until the reasons for the suspension are specified.

4.5.8 RESUMING SUSPENDED CERTIFICATE

Evrotrust resumes the operation of a suspended certificate:

- after dropping the ground for stopping before the end of the suspension;
- upon request of the Signatory, after clarifying the reasons for the suspension requested;

Upon renewal of the certificate, the latter is considered to be valid.

4.6 CHECKING THE STATE OF PLAY (STATUS) OF A QUALIFIED CERTIFICATE

Information on the status of certificates issued by Evrotrust may be obtained from the CRL, published on the Evrotrust website and through the OCSP Online Certificate Verification Protocol.

Authentication services for status verification of Qualified Certificates are available 24/7/365 (continuously operating).

4.7 TERMINATION OF A QUALIFIED CERTIFICATION SERVICES AGREEMENT BY USER

The Contract for Qualified Certification Services between Evrotrust and User is terminated:

- after expiry of the last issued qualified certificate, and the user has not taken any action to update his/her qualified certificate;
- when the qualified certificate has been terminated and the user has not taken action to issue another certificate.
- when User profile is closed from the Evrotrust mobile application. In this case, all qualified certificates issued shall be terminated.

5 CONTROL OF PHYSICAL AND ORGANIZATIONAL SECURITY

5.1 CONTROL OF PHYSICAL SECURITY

The measures taken with regard to the physical protection of Evrotrust are an element of the Evrotrust Information Security System, which complies with the requirements of ISO/IEC 27001:2022, ISO 9001:2015, ISO 22301: 2019, и ISO/IEC 20000-1:2018.

** The measures related to the physical protection of the information data are described in the document "Practice of Qualified Certification Services".*

5.1.1 PREMISES AND THEIR STRUCTURE

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

5.1.2 THE PHYSICAL ACCESS

The physical security of certificate issuing and management systems is consistent with the requirements of international standards and recommendations.

** The physical security procedure is described in the document "Practice of Qualified Certification Services".*

5.1.3 STORAGE OF DATA CARRIERS

All media containing software, data archives, or audit information are stored in a firebox in a special archive room with access control. There is a system of physical and logical protection in the room with Evrotrust’s archive.

5.1.4 WASTE DISPOSAL

Paper and electronic media containing potentially significant security information for Evrotrust shall be destroyed in special shredding devices after the storage period specified in the internal rules.

The data carriers for the cryptographic keys used for their storage and the access codes are fragmented with appropriate devices. This applies to carriers that do not allow the permanent deletion of stored data and its reuse.

In certain cases, information from portable media is destroyed by deleting or formatting the non-recoverable environment.

5.2 ORGANIZATIONAL CONTROL

All security procedures for issuing, administering, and using Qualified Certificates for Advanced Electronic Signature/Seal are performed by trusted Evrotrust staff.

Evrotrust maintains a sufficient number of qualified employees who, at every moment of its activity, ensure compliance with the applicable legislation and the company’s internal rules and regulations.

5.2.1 TRUSTED ROLES

A detailed distribution of the functions and responsibilities of the staff is written in Evrotrust’s internal documents: job descriptions, establishment plan and relevant internal operational procedures.

The allocation of functions is done in such a way as to minimize the risk of compromise, leakage of confidential information or the occurrence of a conflict of interest.

** The procedure for selecting trusted roles is described in the document "Practice of Qualified Certification Services".*

5.2.2 REQUIREMENTS FOR DIVISION OF RESPONSIBILITIES

The trusted activities of Evrotrust personnel are performed by different persons.

5.3 STAFF CONTROL

The staff of Evrotrust consists of a sufficient number of highly qualified employees. Trusted persons have the necessary professional background and experience to ensure that security requirements and technical security assessment standards are respected. Professional knowledge of information systems, cryptography and public key infrastructure enables employees with trusted roles to perform their duties properly.

Evrotrust employees periodically attend further training courses in accordance with the current requirements in Evrotrust’s fields of activity.

5.3.1 REQUIREMENTS FOR THE TRAINING OF EVROTRUST STAFF

Personnel performing functions and tasks arising from their employment in Evrotrust or employment in the Registration Authority (with the presence of an external Registration Authority) must undergo the compulsory training:

** The requirements are described in the document "Practice of Qualified Certification Services".*

5.4 EVENT LOGS AND JOURNAL MAINTENANCE

For the efficient management and operation of Evrotrust, all events having a significant impact on the security and reliability of the technology system, personnel and user control and the security impact of the qualified certification services provided are recorded.

Electronic journal information is generated automatically.

Recordings journals of recorded events are stored in files on the system disk for at least 6 (six) months. During this time, they are available online or in the process of searching by any authorized Evrotrust employee. After this period, the records are stored in the archives.

Archived journals are kept for at least 20 (twenty) years.

The archive is signed with an electronic signature/electronic time stamp. Information from the log entries is periodically recorded on physical media stored in a special safe located in a room with a high degree of physical protection and access control.

5.4.1 VULNERABILITY AND EVALUATION

Evrotrust classifies and maintains registers of all assets in accordance with ISO/IEC 27001: 2022. According to the “Security Policy” of Evrotrust, an analysis is carried out for the vulnerability assessment of all internal procedures, applications and information systems. Analytical requirements may also be determined by an external institution authorized to audit Evrotrust.

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

5.5 ARCHIVING

Information about significant events is archived in electronic form periodically.

Evrotrust backs up all data and files related to: registration information; system security; all requests submitted by users; all consumer information; all keys used by the Certifying Authorities and the Registration Authority; and all correspondence between Evrotrust and users. All documents and data used in the identity verification process are subject to backup.

5.6 TERMINATION OF EVROTRUST OPERATION

5.6.1 REQUIREMENTS RELATING TO THE TRANSITION TO THE TERMINATION OF THE SUPPLIER'S BUSINESS

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

- notify the Supervisory Authority of its intention to terminate its services in the event of an action for declaring the company bankrupt, declaring the company invalid or otherwise requesting termination or initiating winding-up proceedings. The notification should be made 4 (four) months before the agreed date of termination;
- notify (at least 4 months before) its users of the decision to terminate the services it provides;
- changes the status of their certificates;
- terminate all user certificates within the announced end-of-service period;
- notify all its users of termination of services;
- makes commercial reasonable efforts to minimize distortion of consumer interests;
- pays compensation to consumers (compensation must be proportional to the remaining period of validity of the certificates);
- carries out the necessary action to enable the Supervisory Authority to maintain the CRL.

If the decision to terminate the certification service only concerns the Registration Authority, it shall be obliged to:

- notify Evrotrust about its intention to terminate the registration activity. The notification should be made 4 (four) months before the agreed date of termination;
- transmit to the receiving Provider the complete documentation related to the users, including the archive and the audit data.

5.6.2 TRANSFER OF BUSINESS TO ANOTHER QUALIFIED SERVICE PROVIDER

In order to ensure the continuity of the issuance of qualified authentication services to consumers, Evrotrust may sign an agreement with another qualified certification service provider. In this case, Evrotrust shall:

- notify the Supervisory Authority of its intention no later than 4 months before the date of termination and transfer of the business;
- make every effort and care to continue the validity of issued user certificates;
- notify the Surveillance Authority and Consumers in writing that its activity is being undertaken by another registered supplier as well as its name. The notification shall be published on the Evrotrust website;
- notify Users of the Conditions of Maintenance of Transferred Certificates to the Receiving Provider;
- modify the status of the operating certificates and duly transmit all documentation relating to its activity to the receiving Provider, together with all records and all certificates issued (valid, suspended and discontinued);
- perform the necessary actions to transfer the maintenance of the information to the receiving Provider;
- transfer the management of the already issued end-user certificates to the receiving Provider;

The Receiving Provider assumes the rights and obligations of Evrotrust with terminated activity and continues to manage the active Qualified Certificates until the end of their operation.

The Evrotrust Archive with terminated status must be delivered to the Provider accepting the activity.

5.6.3 DISQUALIFICATION OF QUALIFIED PROVIDER OR QUALIFIED SERVICE STATUS

In the event of the revocation of the qualified Evrotrust status or of any of its certification services, it shall:

- notify its users of the changed status of its services;
- change the status of their certificates;
- terminates issuance of new qualified certificates but continues to support and maintain the already active certificates until they expire;
- make commercial reasonable efforts to minimize distortion of consumer interests;

6 MANAGEMENT AND CONTROL OF THE TECHNICAL SECURITY

6.1 GENERATING AND INSTALLING A PAIR OF KEYS OF A CERTIFICATION AUTHORITY

Evrotrust generates pairs of cryptographic (RSA) keys on the base and on the Operations Certification Authorities using an HSM/Hardware Security Module at FIPS 140-2 Level 3 or above, or CC EAL 4+ or higher respectively.

Evrotrust uses its private keys only for its business purposes as follows:

- ➢ to sign the operating certificates issued to the Certification Authorities on its infrastructure;
- ➢ to sign CRLs issued and published;
- ➢ to sign all issued and published Advanced Electronic Signature/Seal Certificates to Users.

6.1.1 GENERATING PAIR OF KEYS TO SIGNATORY/CREATOR

The Signatory/Creator's keys of a Qualified Certificate for Advanced Electronic Signature/Seal are generated in a secure environment as required by Regulation (EU) No. 910/2014.

The control of the private key is through an access code. The Signatory uses the private key to create a signature/seal by entering the code in the secure environment to create an advanced electronic signature/seal.

When the key pair is generated by the Signatory/Creator, Evrotrust recommends that the latter use an approved environment in the Evrotrust infrastructure to create an advanced electronic signature/seal or equivalent that complies with the requirements of Regulation (EU) No. 910/2014 and is compatible with the Evrotrust infrastructure.

In cases where the pair of keys is generated by the Signatory or the Creator, the latter bears full responsibility for the protection of the private key in order to prevent its compromise, disclosure, modification, loss or unauthorized use. The Signatory/Creator is responsible for omissions or actions by authorized persons who are authorized to generate, keep or store their private keys.

The Signatory/Creator undertakes to use licensed software to work with the environment to create an advanced electronic signature/seal.

6.1.1.1 REQUIREMENTS TO THE ENVIRONMENT FOR CREATION OF UPDATED ELECTRONIC SIGNATURE/SEAL

The environment for the creation of an advanced electronic signature/seal shall ensure, by appropriate technical and procedural means, at least that:

- the confidentiality of electronic signature/seal creation data used for the creation of the electronic signature/seal is reasonably guaranteed;
- the data for creating an electronic signature/seal are practically only once met;
- the electronic signature/seal creation data are sufficiently secured and cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
- the electronic signature creation data may be reliably protected by the legitimate Signatory/Creator of the signature/seal against use by others.

Advanced electronic signature/seal creation environment shall not alter the data to be signed or prevent such data from being presented to the Signatory/Creator prior to signing.

Generating or management of data for creating an electronic signature/seal on behalf of the Signatory/Creator of the electronic signature/seal can only be carried out by Evrotrust.

6.1.1.2 REMOTE GENERATION OF A PAIR OF KEYS

The Creator/Signatory uses specialized software provided by Evrotrust, which implements the process of generating and managing the cryptographic pair of keys.

The generation, use, and storage of the private key has a high level of security that is guaranteed by the environment where it is created. It is securely protected and accessed only by the Signatory/Creator or an authorized representative of the legal entity.

The Creator/Signatory or Authorized Representative of the legal entity generates an electronic application for a Qualified Certificate in PKCS # 10 format and sends it to Evrotrust. According to the recommendations of RFC 2314 - PKCS # 10, ASN.1, the electronic request form contains a DN, a public key and other attributes, all of which are signed with the private key.

When remote generation of the key pair is performed where requested by the Evrotrust mobile application, it is generated in a reliable Evrotrust environment that meets the requirements of the Advanced Electronic Signature Environment Regulation.

6.1.1.3 DELIVERY OF A PRIVATE KEY TO A USER

When the key pair is generated at Evrotrust, the Signatory/Creator or the authorized representative of the legal entity receives the private key and the qualified certificate issued at the supplier's Registration Authority or electronically.

The initial User and Administrative Access Code is provided to the Signatory/Creator or the authorized representative of the legal entity in a stamped, opaque paper envelope or alternative electronic channel.

When remote generation of the key pair takes place, the private key is generated and stored encrypted in a reliable Evrotrust environment. The key encryption is a PIN-code created by the Signatory/Creator, which ensures that only he can be accessed to activate the key.

6.1.2 DELIVERY OF A PUBLIC KEY FROM A VENDOR USER

It is executed only by the Signatory/Creator or an authorized representative of a legal entity in which a pair of keys is generated and who is to deliver its public key to Evrotrust for the purposes of the process of issuing a qualified certificate.

The Signatory/Creator or authorized representative of the legal entity delivers, via the Evrotrust registration authority, the public key of the generated pair of keys, by means of a request in electronic form, whose format is PKCS # 10. The request contains a public key and is signed electronically with the corresponding private key.

The user may submit the electronic application on a medium or electronically to the Registration Authority together with the other documents under the Evrotrust Policy or through the Evrotrust webpage.

The registration authority of Evrotrust must verify the holding of the private key by the Signatory/Creator or the authorized representative of the legal entity and confirm the request for a qualified certificate.

This procedure is not implemented when remote certificates are applied through the Evrotrust mobile application.

6.1.3 KEY LENGTH

The length of a pair of keys for Enhanced Electronic Signature/Seal of a User Generated through the Evrotrust infrastructure can be 2048, 3072 or 4096 bits, with an applicable combination of asymmetric and hash algorithms: sha256-with-RSA.

Regardless of where the pair of keys for certificate issuance for advanced electronic signature/ seal is generated, the key must be at least 1024 bits long for RSA and DSA algorithms and 160 bits for ECDSA algorithms.

6.1.4 PUBLIC KEY PARAMETERS

The Signatory/Creator or Authorized Representative of the legal entity of a key pair is responsible for verifying the quality of the generated private key parameters. It is required to verify the ability of the key to encrypt and decrypt, including creating an electronic signature and performing a check.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE CONTROL

Each User creates and stores a private key using a reliable system for its security. The Certification Authority generates a pair of keys upon request from the User and transmits it to a secured state by notifying him of the rules for storing and protecting his private key.

6.2.1 CONTROLLING OF USE AND STORAGE OF A PRIVATE KEY

The private key of the Signatory/Creator or the authorized representative of the legal entity is only used in a secure environment to create an advanced electronic signature/seal, as required by Regulation (EU) No. 910/2014.

Evrotrust does not in any way store or archive a private key of a User to create an electronic signature/seal, except in the case of remote certification of a qualified certificate through the Evrotrust mobile application. In this case, the private key is generated and stored encrypted in a reliable Evrotrust environment. The key encryption is a PIN-code created by the Signatory/Creator, which ensures that only he can be accessed to activate the key.

6.2.2 PRIVATE KEY STORAGE

Evrotrust does not create copies of users' private keys except in the case of the previous paragraph. If the private key is deleted or lost, the user must replace it and request the issuance of a new qualified certificate.

6.2.3 PRIVATE KEY ACTIVATION METHOD

The private key of the Signatory/Creator or an authorized representative of the legal entity is activated by entering the user code to access where the key is stored securely or using another means of identification with the same or higher security level.

6.2.4 METHOD FOR DISABLING A PRIVATE KEY

A private key of Signatory/Creator or an authorized representative of the legal entity is deactivated by deleting the private key or destroying the environment where it is stored. This will permanently disable the access and use of the private key.

6.2.5 PRIVATE KEY DESTROYING METHOD

The private key of a Qualified User Certificate is destroyed by deleting it from the environment where it is stored or by physical destruction.

6.3 OTHER ASPECTS OF PAIR KEY MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVING

Public Keys of Signatories/Creators or authorized representatives of legal entities are contained in the Qualified Certificates issued to them, which are published in the Register of certificates of the Evrotrust Web site and stored in a repository.

6.3.2 PERIOD OF VALIDITY OF QUALIFIED CERTIFICATE AND USE OF KEYS

The period of use of public keys is determined by the value of the field in the certificate describing the validity of the public key. The validity of the certificates and their respective private keys may be curtailed in the event of termination of the certificates.

6.4 ACTIVATION DATA

When the User is personally present at the Registration Authority, the activation data of a private key are primarily used by the operator of the Registration Authority. Users use authentication and control access to their private key.

In cases where the Signatory/Creator or the authorized representative of a legal entity generates a pair of Qualified Certificate Keys, they create and manage the activation data themselves.

6.4.1 GENERATING AND INSTALLING ACTIVATION DATA

Activation data is used during initial issuance of a certificate in an environment to create an advanced electronic signature/seal before generating a pair of keys.

Access codes and environment unblocking to create an advanced electronic signature/seal are provided to the Signatory/Creator or the authorized representative of the legal entity in a stamped, opaque paper envelope or in an electronic form on an alternative channel.

When using a mobile application of Evrotrust, the access code is generated by the Signatory/Creator. The code is not stored by Evrotrust and can only be accessed by the user while the mobile application is activated. To recover the personal code, the Signatory/Creator creates a special crypto-key that is generated by secret word by the user at the time of registration via the mobile application. The pin code and the secret word are not kept by Evrotrust.

6.4.2 PROTECTION OF ACTIVATION DATA

The Signatory/Creator or Authorized Representative of the legal entity is required to store and protect from compromising the access codes to the environment to create an advanced electronic signature/seal.

Evrotrust recommends that environment activation data never be stored in the environment itself.

6.5 COMPUTER SYSTEMS SECURITY

Evrotrust only uses reliable and secure hardware and software that are part of the Evrotrust computer system.

The computer systems that operate all critical components of the Evrotrust infrastructure are equipped and configured with means of locally protecting software and information data access.

Evrotrust uses procedures to manage the information security of the entire Evrotrust infrastructure in accordance with generally accepted international practice standards.

6.6 LIFE CYCLE SECURITY OF THE TECHNOLOGY SYSTEM

All hardware changes are monitored and registered by authorized Evrotrust staff. When purchasing new technical equipment, it is supplied with the necessary operating procedures and instructions for use.

Supervision of the functionality of the technological system is ensured and it is ensured that it functions properly and in accordance with the delivered manufacturing configuration.

6.7 NETWORK SECURITY

Evrotrust infrastructure utilizes modern technical means of information exchange and protection to ensure the network security of systems against external interventions and threats.

7 PROFILES OF QUALIFIED CERTIFICATES FOR ADVANCED ELECTRONIC SIGNATURES/SEALS

User Qualified Certificates profiles comply with the format described in ITU-T X.509 v.3 standard. A certificate of type X.509 v.3 is a data set that uniquely authenticates the public key to the author of the advanced electronic signature/seal.

** Profiles of: Qualified Natural Person Certificate for AES (Qualified Certificate of Enhanced Electronic Signature for Individuals); Qualified Enhanced Legal Entity Certificate for a Legal Entity ("Evrotrust Qualified Legal Person Certificate for AESeal"); A Qualified PSD2 Certificate for Advanced Electronic Seal of a Legal Entity ("Evrotrust Qualified PSD2 Legal Person Certificate for AESeal") is described in the document "Practice of Qualified Certification Services".*

8 VERIFICATION AND CONTROL OF SUPPLIER'S ACTIVITY

The audits carried out at Evrotrust concerns the processing of information data and management of key procedures.

Evrotrust annually performs at least one internal audit.

Evrotrust is audited at least once every 24 months by a Compliance Assessment Body. The purpose of the audit is to confirm that the Qualified Certification Services Provider and the Qualified Certification Services Providers comply with the requirements set out in Regulation (EU) No. 910/2014.

8.1 ACTIONS TAKEN AS A RESULT OF AN AUDIT

Reports of internal and external audits are transmitted to Evrotrust.

The report of the Compliance Assessment Body shall be transmitted to the Supervisory Body within 3 (three) days of its handing over to the Evrotrust management. The Supervisory Authority examines the report and decides whether to leave or take the qualified Evrotrust status.

On the basis of the assessments made in the report, Evrotrust's Guide sets out measures and deadlines for remedying the identified gaps and inconsistencies.

Evrotrust staff undertake specific actions for their removal within the specified deadlines.

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 PRICES AND FEES

Evrotrust maintains the document "Pricing for certification, information, cryptographic and consultancy services" on its website: https://www.evrotrust.com/.

9.1.1 RETURN OF A CERTIFICATE AND REIMBURSEMENT OF PAYMENT

Signatory/Creator or authorized representative of a legal entity may object to an inaccuracy or incompleteness in the content of a qualified certificate issued within 3 days after its publication in the Register of issued certificates.

If the reason for the false content of a qualified certificate is in the Registration Authority, Evrotrust terminates the certificate and issues a new one with true content on its own account or refunds the payment for the revoked certificate with false content.

If the reason for the false content of a qualified certificate is due to the Signatory/Creator or the authorized representative of a legal entity, Evrotrust shall terminate the certificate and shall not reimburse the payment made. Evrotrust may issue a new one with true content at the expense of the User.

The user may refuse to issue a qualified certificate of true content that Evrotrust will terminate immediately without reimbursing the payment for the revoked certificate.

9.2 FINANCIAL RESPONSIBILITIES

Evrotrust is responsible for the certification services provided to the users who rely on the certificates.

Evrotrust shall be liable if the damage is due to his fault or fault of the persons to whom he has assigned the job.

If Evrotrust confirms and accepts that damage has occurred, it undertakes to pay the remedy. The maximum payment limit may not exceed the amount of the damage.

9.2.1 ACTIVITY INSURANCE

Evrotrust undertakes compulsory insurance of its activity as a registered Provider of Qualified Certification Services.

9.3 PRIVACY OF PERSONAL DATA

Evrotrust is registered as an administrator of personal data under the terms of the Personal Data Protection Act.

As a Personal Data Administrator, Evrotrust strictly observes the requirements of confidentiality and non-dissemination of the personal data of Signatory/Creator or authorized representatives of legal entities that have become known to it in its capacity of Qualified Certification Services Provider.

9.4 INTELLECTUAL PROPERTY RIGHTS

Various data included in the Evrotrust qualified certificates or published in the Register/Repository are subject to intellectual property rights and other proprietary and non-material rights.

9.4.1 OWNERSHIP OF A PAIR OF KEYS

The user key pair and the associated public key certificate issued by Evrotrust, as well as the relevant secret material, are owned by Evrotrust, regardless of the ownership of the physical environment in which the keys are stored and protected.

9.5 OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF EVROTRUST

Evrotrust ensures that it carries out its activities as:

- strictly complies with the terms of this document, the requirements of Regulation (EU)

No. 910/2014 and the national legislation in the performance of its activity as Qualified Certification Services Provider;

- the services provided do not infringe the copyrights and licensed rights of third parties;
- uses technical equipment and Technologies that ensure system reliability and technical and cryptographic security in the process, including a secure and secure mechanism/environment for generating keys and for creating an advanced electronic signature/seal in its infrastructure;
- issues qualified certificates for electronic signatures/seal after verifying the information provided by law;
- securely stores and maintains information related to the certificates issued and the systems operation;
- complies with the established operating procedures and technical and physical control rules, in accordance with the terms of this Policy and "Practice in Providing Qualified Certification Services";
- creates an opportunity for immediate suspension and termination of a qualified certificate;
- terminates and suspends the performance of certificates under the terms and conditions of the relevant Policy;
- immediately informs the interested parties after the suspension of a qualified certificate;
- provides conditions for accurately determining the timing of issuance, suspension, resumption and termination of Qualified Certificates;
- performs procedures for identification and authentication of the Signatory/Creator or the authorized representative of a legal entity;
- provides measures against tampering with qualified certificates and the confidentiality of the data accessed in the process of creating the advanced electronic signature/seal;
- uses reliable systems for storing and managing certificates;
- only duly empowered employees have access to make changes to the data, establish the authenticity and validity of the certificates;
- takes immediate action in the event of technical security issues;

- upon expiration of the validity of a qualified certificate, cancels its validity;
- informs the Signatories/Creators or authorized representatives of legal entities as well as the Relying Parties about their obligations and due diligence in the use and trust of the qualified certification services provided by Evrotrust as well as the correct and safe use of the issued Qualified Certificates and the Certification Related services;
- uses and stores the collected personal and other information solely for the purposes of its activity of providing qualified certification services in accordance with national law;
- does not store or copy data to create custom private keys except for remotely requesting Qualified Certificates through the Evrotrust mobile application;
- maintains disposable means that enable it to carry out its activities;
- concludes insurance policy for the time of its activity;
- maintains trusted staff with the necessary expertise, experience and qualification to perform the activity;
- maintains a repository in which it publishes the issued Qualified Certificates, a current CRL, other circumstances and electronic documents under this Policy and national legislation;
- provides permanent access to the repository electronically (24/7/365);
- provides protection against making changes to the maintained repository from unauthorized or unauthorized access or due to a random event;
- immediately publishes in the Register of certificates the certificates issued and signed;
- creates the conditions for each relying party to verify the status of issued and published qualified certificate in the Register of Certificates;
- performs periodic internal audits of the activity of the Certifying 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 user hardware, forms, Forms, Types of Contract and other documents for the benefit of users;

Evrotrust is liable to Users and Trustees for damages caused by gross negligence or intent:

- by failure to meet the requirements of Regulation (EU) No. 910/2014 in the performance of its activity of providing qualified certification services;
- from false or missing data in the Qualified Certificate at the time of issue;
- from damages caused if, during the issuance of the Qualified Certificate, the person named as Signatory/Creator or authorized representative of a legal entity did not have the private key corresponding to the public key;
- from algorithmic discrepancy between the private key and the public key entered in the Qualified Certificate;
- from non-compliance with its obligations to issue and manage qualified certificates;
- From omissions in establishing the identity of the Signatory/Creator or the authorized representative of a legal entity.

9.5.1 OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF THE REGISTRATION AUTHORITY

Evrotrust ensures that the Registration Authority performs its functions and duties in full compliance with the terms of this document, 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 ensures that the Registration Authority:

- performs its business using reliable and secure devices and software;
- provides services that are in accordance with national law and does not infringe the copyrights and licensed rights of Users;
- makes the necessary efforts to perform correct User identification, correctly and accurately inputs the data in the Evrotrust database and updates this information at the time of validation of the data;
- does not make any deliberate mistakes or misinterpret the information contained in Qualified Certificates;
- its services comply with generally accepted standards: X.509, PKCS # 10, PKCS # 7, PKCS # 12.

9.6 OBLIGATIONS OF USERS

The Signatory/Creator or authorized representative of a legal person specified in the issued qualified certificate as Signatory has the following obligations:

- to become aware with and comply with the terms of the Contract, the Policies and Practices in the provision of qualified certification services by Evrotrust, as well as the requirements in the other documents published on the Evrotrust website;
- when submitting requests for the issuance and management of qualified certificates, to provide true, accurate and complete information that Evrotrust requires under the Contract, the regulatory requirements, the applicable Policies and Practices;
- to generate cryptographic keys using a secure method and algorithm in accordance with the requirements of Regulation (EU) No 910/2014 and to use a secure environment for creating an advanced electronic signature/seal;
- to verify the completeness and authenticity of the content of the authentication information provided by it in the Distinguished Name (DN) field of the Qualified Certificates issued. In case of a discrepancy between the submitted information and the certified content, the user must immediately notify Evrotrust;
- to discontinue the use of a qualified certificate in the event of any doubt about the loss or compromise of the private key and to file an application for termination with Evrotrust;
- to discontinue the use of a qualified certificate in the presence of obsolete, altered, inaccurate and / or incorrect information in it and to file a request for suspension of the certificate;
- 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 qualified certificate issued by Evrotrust for legitimate purposes only and in accordance with the policy and practice specified therein;
- to approve the conditions specified in the Agreement between him and Evrotrust (this approval must be a handwritten signature on the Contract);
- to approve the qualified certificate issued to him/her;
- not to disclose the password to access the environment to create an advanced electronic signature/seal to unauthorized persons;
- not make his/her private key available to others.

9.7 DISCLAIMER

Evrotrust is not responsible for any damages caused by:

- use of a qualified certificate outside the limits of the intended purposes and limitations of its validity;
- Illegal actions by Consumers and Leading Parties;
- providing method for identification of the environment for creating advanced electronic signature/seal and private key access by Third Party Users;
- incidental events of a force majeure, including malicious actions of third parties (hacker attacks, removal of the environment for creating an advanced electronic signature/seal, access to the private key, knowing without the Signatory/Creator of the identification method, etc.)
- use of a qualified certificate that has not been issued or used in accordance with the requirements and procedures of Evrotrust's Practice and Policy;
- use of an invalid certificate (certificate that has been suspended or terminated);
- not timely action to terminate or suspend a certificate (due to a delay by the Signatory/Creator's request or for reasons beyond the control of Evrotrust);
- compromised private key corresponding to the public key in the qualified certificate by fault of the Signatory/Creator;
- poor quality and functionality of the software products and hardware devices used by Signatory/Creator and Relying parties.
- Evrotrust is not responsible for using the certificate beyond the limits of the transaction value limits and usage goals.
- 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 SIGNATORY'S / CREATOR'S RESPONSIBILITY

The responsibility of the Signatory/Creator or the authorized representative of a legal entity results from the performance of his/her duties. The terms of liability are governed by a Contract with Evrotrust.

The Signatory/Creator or Authorized Representative of a Legal Person is liable to Evrotrust and to the Relying parties if:

- in creating the private-public key pair used an algorithm and environment to create an advanced electronic signature/seal that does not comply with the requirements of Regulation (EU) No. 910/2014;

- does not exactly comply with the security requirements set by Evrotrust;
- does not request Evrotrust to suspend or terminate the Qualified Certificate after learning that the private key has been misused or threatened by improper use;
- has made false statements made to Evrotrust relating to the content or issuance of the Qualified Certificate;
- when the qualified certificate is issued with a registered Creator and his authorized person (Signatory), he is responsible for the failure of the authorized person to fulfil his obligations.

Subscriber, Titular/ Creator or the representative of the legal entity is responsible for the content of the attachments and the consequences of their use.

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.