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

CERTIFICATE POLICY

FOR QUALIFIED CERTIFICATION SERVICES

FOR QUALIFIED ELECTRONIC SIGNATURE/SEAL

TABLE OF CONTENTS

1 INTRODUCTION

"Certificate Policy for qualified certification services for qualified 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 qualified electronic signatures/seals, the types of qualified certification services applicable for those certificates, as well as their scope of application.

When issuing a qualified certificate for a qualified electronic signature/seal by Evrotrust, procedures are applied that ensure high level of reliability and security of the certified information identifying the Users. Procedures are applied which guarantee reliability and security when issuing, publishing and managing (suspension, resumption, termination and renewal) qualified certificates, in the creation of a signature/seal, when storing a private key and using it in different applications.

Becoming familiar with the purposes and role of the "Certificate Policy for qualified certification services for qualified electronic signature/seal" is especially important for the Users (Signatories/Creators) and Relying Parties from the point of view of the applicability of these services.

The relations between Evrotrust and the User are regulated by a contract for qualified certification services.

The prices of the certificates and services for the issuance and management of qualified certificates are included in the Evrotrust Price Schedule available on its website.

1.1 REVIEW

The document "Certificate Policy for qualified certification services for qualified electronic signature/seal" refers to qualified certificates issued by Evrotrust in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23/07/2014 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.

The present document is structured according to the framework established with the

recommendation IETF RFC 3647 „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

1.2 LEGAL REFERENCES

The policy is in line 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 319 412-5: „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".

The issuance of qualified certificates for qualified electronic signatures/seals is related to:

- the issuance of a qualified certificate to a natural person (Signatory) – its nature is of a qualified certificate for a qualified electronic signature;
- qualified electronic seal of a legal entity (Creator of a seal) – its nature is of a qualified certificate for a qualified electronic seal.

The "Certificate Policy for qualified certification services for qualified electronic signature/seal" of "Evrotrust Technologies" AD is a public document. It can be modified at any time by Evrotrust and each new version will be communicated to the interested parties by publishing it on the Evrotrust website: https://www.evrotrust.com.

1.3 DENOMINATION AND IDENTIFIER OF THE POLICY

The full title of the present document is "Certificate Policy for qualified certification services for qualified electronic signature/seal" by "Evrotrust Technologies" AD.

The certificates contain a policy identified which can be used by the Relying Parties in

determining their applicability to a given application, as described in the recommendation IETF RFC 3647.

The identifiers for the policies of the qualified certificates specified in the present document are:

QCP-n-qscd:

Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

QCP-l-qscd:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)

Evrotrust maintains and applies a Qualified Certificate Policy which is based on rules established in ETSI EN 319 411-1, with object identifier (OID – Object Identifier), as follows:

Certificate type	Object identifier
Evrotrust Qualified Natural Person Certificate for QES QCP-n-qscd	1.3.6.1.4.1.47272.2.2 *(in line with policy with O.I.D. = 0.4.0.194112.1.2)*
Evrotrust Qualified Legal Person Certificate for QESeal QCP-l-qscd	1.3.6.1.4.1.47272.2.3 *(in line with policy with O.I.D. = 0.4.0.194112.1.3)*
Evrotrust Qualified Natural Person Attribute Certificate for QES QCP-n-qscd	1.3.6.1.4.1.47272.2.2.1 *(in line with policy with O.I.D. = 0.4.0.194112.1.2)*

Evrotrust ensures that it does not alter the object identifier of this document as well as the object identifiers of policies, practices and other referral documents in any circumstances. Evrotrust follows an internal OID management procedure.

1.4 PARTICIPANTS IN THE INFRASTRUCTURE

Evrotrust, as a qualified provider of qualified certification services, provides services for the generation and management (suspension, resumption and termination) of qualified certificates through the Certification Authority "Evrotrust RSA Operational CA", and services for identification of Users through a Registration Authority. Other participants in Evrotrust's infrastructure are Users and Relying Parties.

- **Certifying authority** - "Evrotrust RSA Operational CA" is a certifying authority issuing qualified certificates for qualified electronic signatures/seals managed according to the present policy.
- **Registration authority** - the registering authority is a distinct unit of Evrotrust, but can also be an external legal entity to which Evrotrust assigns to carry out services for registration, identification and certification of the identity of Evrotrust users.

Information for contact with the Registering body of Evrotrust is available on the Evrotrust website.

1.4.1 USERS

Any natural person or legal entity that has signed a contract with Evrotrust is a user of qualified certification services provided by Evrotrust.

The users can be:

- a physical person (Signatory) who creates a qualified electronic signature;
- a physical person (Signatory) who is an authorized representative of a legal entity and creates a qualified electronic signature;
- a legal entity (Creator of a seal) which creates a qualified electronic seal.

When this is practicable, the certification services provided and the products used when providing these services are accessible for people with disabilities.

1.4.2 RELYING PARTIES

A relying party is a natural person or legal entity that accepts a qualified certificate issued

by the Evrotrust infrastructure, after verification of a qualified signature/seal of a User of Evrotrust's qualified certifying services.

1.5 USE AND APPLICABILITY OF QUALIFIED CERTIFICATES

1.5.1 USAGE

A Qualified Electronic Signature / Seal Certificate, Qualified Electronic Time Stamp or Website Authenticity is issued by Evrotrust Technologies AD as a qualified provider of Qualified Certification Services and meets the requirements set out in Regulation (EU) 910/2014.

Qualified certificates allow individuals to use the presumption of certain facts when participating in electronic transactions. They can be used when it is necessary to protect an exchange of electronic information.

A qualified public key certificate is signed by a Evrotrust electronic document in the X.509 standard containing the requisites required by Regulation (EC) No 910/2014 certifying the relationship between the Holder / Creator and his public key corresponding to the private key, The Holder / Creator has created the electronic signature / seal and serves to check the signature / seal on electronic documents and other electronic objects.

Qualified certificates issued by Evrotrust can be used to authenticate and create a high level of trust about the authorship / source and integrity of a particular electronic object. Consumers should be aware of the requirements for issuing certificates and formulate an application to Evrotrust in order to issue an appropriate certificate for these purposes. When providing incorrect information to consumers, they are responsible.

Certificates issued and provided by Evrotrust can be used to:

- Identity and identity identification of a natural person or an individual related to an organization, acting as its legal or contractual agent, by attribute certificates;
- Authentication link between the author and his / her public key for checking the authorship and integrity of electronically signed documents;
- Authentication of a website with which a visitor to a website can be confident that the website owner is a real and legitimate subject, as well as to ensure a secure communication session with the website under a standardized protocol;
- Evidence that an electronic document or other information object proceeds from a

legal entity, ensuring the reliable origin and integrity of the object, by means of an electronic seal accompanied by an electronic seal certificate issued by Evrotrust;

- Signing, encryption and decryption of electronic data, such as electronic documents, databases, information objects and others;
- Verification of signed data, such as documents and others;
- Encryption and decryption of data and exchange of keys used for encryption;
- Secure remote storage and use of keys for electronic signing;
- Others.

1.5.2 RECOMMENDATION FOR THE APPLICABILITY OF SPECIES QUALIFIED CERTIFICATES

A qualified certificate of a natural person (Signatory)/legal entity (Creator) or authorized representative of a legal entity, specified as Signatory in the certificate, can be used when creating a qualified electronic signature/seal in electronic documents and applications/transactions requiring the highest level of information security.

Applicability of different types of qualified certificates:

- Qualified certificates for electronic signature of individuals - these certificates allow the electronic signing of electronic documents (PDF (PaDES), XML (XaDES), TXT (CaDES), etc.), including document packages (ASiC-E);
- Qualified certificates for electronic seal of legal entities / organizations - they allow electronic signing of different assets of the company / organization by e-seal, like - pictures, software, video, etc .;
- SSL (Secure Socket Layer) qualified server verification certificates - they are used by global Internet or extranet services operating on SSL / TLS protocol;
- Qualified certificates used to verify the authenticity of individuals and legal entities - used for example in SSL / TLS / protocol;
- Qualified certificates confirming the status of certificates - issued to servers operating in accordance with the OCSP protocol;
- Qualified electronic time stamps - they are issued on servers in response to a request for timing;

- Other - for example attribute certificates certifying certain attributes / attributes of a person or object.

1.5.3 PROHIBITION FOR THE USE OF QUALIFIED CERTIFICATES

Evrotrust qualified certificates should not be used in a manner incompatible with their declared purpose and their field of application/Policy.

The qualified certificates issued in accordance herewith should not be used for unlawful purposes.

1.6 MANAGEMENT OF THE POLICY

1.6.1 ORGANIZATION MANAGING THE POLICY

Evrotrust is responsible for the management of this Policy.

Each version of the Policy will be in force till the moment of approval and publication of the new version. Each new version will be developed by Evrotrust's employees and published after approval by Evrotrust's Board of Directors.

The users should follow only the Policy version in force as of the time when Evrotrust services are used.

1.6.2 CONTACT PERSON

The contact person for the management of the document ""Certificate Policy for qualified certification services for qualified electronic signature/seal" by "Evrotrust Technologies" AD is the executive director or Evrotrust.

Additional information can be obtained at the following address:

"Evrotrust Technologies" AD

Sofia, 1766

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

Telephone, Fax: + 359 2 448 58 58

Email: office@evrotrust.com

1.6.3 CONNECTION BETWEEN THE POLICY AND THE PRACTICE

The ""Certificate Policy for qualified certification services for qualified 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 qualified electronic signature/seal issued by Evrotrust.

The main difference between the two documents is in the focus of their provisions and in their targeted purpose. The Policy reviews the requirements and implementation of the standards imposed by the created Evrotrust infrastructure and determines the participants in the activities for providing certification services. The Practice, on the other hand, indicates how the Certifying Authority and the other participants in the infrastructure apply the procedures and controls, in order to fulfil the Policy requirements. In other words, the goal of both documents is to ensure uniformity of the rules and procedures, how the participants in the Evrotrust infrastructure fulfil their obligations and responsibilities.

The main difference between the Policy and the Practice is that the Certifying Authority can support several Policies with one Practice, policies which are used for different applications or with a different application area for different Relying Parties.

1.7 DEFINITIONS AND ABBREVIATIONS

1.7.1 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 used by the Signatory of the

electronic signature for the creation of an electronic signature;

Relying Parties - Natural persons or legal entities that are addressees of electronic statements and other information objects and rely on Evrotrust's certifying services;

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 format which tie other data in electronic format to a specific moment in time and serve as proof that this data existed at the respective moment and was issued in accordance with Regulation (EU) No 910/2014;

Electronic seal - Data in electronic format that are added to other data in electronic form or are logically tied to them, so as to guarantee the origin or integrity of the latter. The electronic seal serves as proof that a given electronic document was issued by a legal entity and guarantees the reliable origin and integrity of the data;

Electronic signature - Data in electronic format which are added to other data in electronic format or are logically tied to them used by the electronic signature signatory to sign;

Qualified certification service - Certification service that meets the corresponding requirements established in Regulation (EU) No 910/2014;

Qualified certification for electronic signature – Certification for electronic signature issued by a supplier of qualified certification services meeting the prerequisites provided in Regulation (EU) No 910/2014;

Qualified time stamp – Electronic time stamp that meets the requirements provided in Regulation (EU) No 910/2014;

Qualified electronic seal - The qualified electronic seal is an improved electronic seal created by a device for the creation of qualified electronic seals and it is based on a qualified certificate for electronic seal;

Qualified electronic signature - An improved electronic signature created by a device for the creation of a qualified electronic signature and it is based on a qualified certificate for electronic signature;

Coordinated Universal Time/UTC – Hour time with respect to which the time in the different time zones is calculated. The international atomic time (TAI) is used as the basis for it;

Policy Approval Authority/PAA – A body authorized to approve, monitor and support the Certification Policy;

Body for evaluation of compliance - A body accredited in accordance with Regulation (EC) No 765/2008 as competent to carry out evaluation of the compliance of a provider of qualified certification services, and of the qualified certification services provided by this provider with respect to 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;

List of suspended or terminated certificates (CRL/Certificate Revocation List) – The list contains certificates which can no longer be deemed to be valid; CRL is digitally signed by the issuer of the certificates – the Certification Authority;

Creator of a seal - A legal entity which creates an electronic seal;

Private key – A sequence of symbols used in an algorithm for transforming information from understandable into encrypted type or vice-versa – from encrypted into understandable type (decryption);

Public key –One of a pair of keys used in an asymmetric cryptosystem which is accessible and can be used for verification of an electronic signature/seal;

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

Certificate of electronic seal – A certificate of a legal entity, by virtue of Regulation (EU) No 910/2014;

Time stamp certificate - Data in electronic format which tie other electronic data to a specific moment of time, providing proof that these data existed as of a given moment;

Electronic signature certificate - Electronic proof that ties the data for validation of an electronic signature to a natural person and, at the least, confirms the name and alias of this person;

Device for the creation of qualified electronic seal - A device for the creation of qualified electronic seal is a device for the creation of electronic seal which meets the requirements of Regulation (EU) № 910/2014;

Device for the creation of qualified electronic signature - A device for the creation of a qualified electronic signature is a device for the creation of electronic signature which meets the requirements of Regulation (EU) № 910/2014;

Device for the creation of electronic signature - A device for the creation of electronic signature is a configured software or hardware used to create electronic signature.

1.7.2 ABBREVIATIONS

QCP-l-qscd – Policy for a qualified certificate issued to a legal entity when the private key of the certificate related to it was generated with QSCD;

QCP-n-qscd – Policy for a qualified certificate issued to a natural person when the private key of the certificate related to him/her was generated with QSCD**;**

QSCD – Device for the creation of qualified electronic signature/seal;

NCP+ - Enhanced normalized certifying policy which 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 - Policy for providing qualified certificates for qualified electronic signature/seal;

CPS Certification Practice Statement - Practice for providing certification services;

CRL, Certificate Revocation List - A list of suspended and terminated certificates;

DN, Distinguished Name - Distinguishing name of a subject recorded in the certificate;

Enhanced key usage - Widened purposes for using the key;

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

HSM, Hardware Security Module - Hardware cryptographic module;

Issuer

LDAP, Lightweight Directory Access Protocol A protocol for simplified access to a register;

OID, Object Identifier;

PKCS, Public Key Cryptography Standards - Cryptographic standard for the transmission of a public key;

PKI, Public Key Infrastructure - Infrastructure of the public key – the totality of the hardware, software, personnel, documentation in Evrotrust for the creation, use, management and verification of issued certificates for electronic signatures/seals;

RA, Registration Authority – Registering Authority;

RSA, Rivest-Shamir-Adelman - A type of asymmetric cryptographic algorithm for the creation of an electronic signature;

SHA, Secure Hash Algorithm - A secure hash-algorithm for extracting a hash-identifier;

SSL, Secure Socket Layer - Secure channel for data transmission;

SMIME, Secure Multipurpose Internet Mail Extensions - Protocol for the secure transmission of email through the Internet.

2 RESPONSIBILITY FOR PUBLICATION AND REPOSITORY

2.1 REPOSITORY

Evrotrust maintains a repository in which current and previous versions of electronic documents (including the current version of the ""Certificate Policy for qualified certification services for qualified electronic signature/seal" and "Practice for providing 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 relying parties have continuous access to the entire information in the repository at the address: https://www.evrotrust.com.

2.2 PUBLISHED INFORMATION

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

The issued qualified certificates are stored in a database of Evrotrust. Access to these certificates can be realized through online protocol for verification of the status of the issued certificates in real time OCSP (Online Certificate Status Protocol).

For online verification of data from the register it is necessary to use suitable software (OCSP-client or access through the provider's webpage).

Verification of issued qualified certificates can be done also in the List with suspended or terminated certificates (CRL) which is published on the website of Evrotrust and is updated every 3 (three) hours.

2.3 FREQUENCY OF PUBLICATION

The documentation including Policy and Practice for providing qualified certification services, agreements, specimens, manuals for work with electronic signature/seal, audit reports, etc., issued by Evrotrust, is published on the Evrotrust webpage immediately during each update.

The operative certificates of the Certifying Authority are published immediately with each issuance of new certificates.

Updates of the Register of certificates with the issued user qualified certificates are performed automatically and immediately after publishing each newly-issued valid certificate.

An update of the current List of suspended and terminated certificates (CRL) is performed automatically no more than 3 (three) hours or immediately after the cancellation or suspension/restoration of a valid certificate.

2.4 ACCESS TO PUBLICATIONS

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

The access to the information in the repository is not restricted by Evrotrust, unless requested by the Signatory/Creator, and only in relation with his valid issued qualified certificate.

The information published in the Evrotrust repository is accessible continuously (24/7/365), except in the cases of events beyond the control of Evrotrust.

3 IDENTIFICATION AND VERIFICATION OF IDENTITY

3.1 NAMES*

The requirements for the names in the certificates are in accordance with ETSI EN 319 411-1, clauses 6.2.1 and 6.6.1 of ETSI EN 319 411-2. Eurotruck has complied with the provisions of ITU-T X.509 or IETF RFC 5280 and ETSI EN 319 412. It is allowed that the names are in accordance with the Domain Name Service (DNS) described in RFC 2247.

** A detailed description of the requirements for the names in Qualified Certificates is provided in the Practice of Qualified Certification Services.*

3.2 INITIAL REGISTRATION*

** The identity verification procedure is described in the Practice of Qualified Certification Services.*

3.2.1 VERIFICATION OF THE POSSESSION OF A PRIVATE KEY*

** The identity verification procedure is described in the Practice of Qualified Certification Services.*

3.3 VERIFICATION OF THE IDENTITY OF A LEGAL ENTITY*

Evrotrust applies the requirements set out in clause 6.2.2 of ETSI EN 319 411-1.

** The identity verification procedure is described in the Practice of Qualified Certification Services.*

3.4 ESTABLISHING THE IDENTITY OF A NATURAL PERSON, AN AUTHORIZED REPRESENTATIVE OR A LEGAL ENTITY*

Evrotrust applies the requirements set out in clause 6.2.2 of ETSI EN 319 411-1.

* The identity verification procedure is described in the Practice of Qualified Certification Services.

3.5 ESTABLISHING THE IDENTITY OF A NATURAL PERSON*

Evrotrust applies the requirements set out in clause 6.2.2 of ETSI EN 319 411-1.

** The identity verification procedure is described in the Practice of Qualified Certification Services.*

3.6 VERIFICATION BY THE CERTIFYING AUTHORITY

After 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 before the Certifying Authority. The Certifying Authority publishes immediately the issued qualified certificate in the Register (database) of issued certificates or, respectively, in the list of suspended and terminated certificates (CRL).

In Evrotrust only the operating Certifying Authority that issued the qualified certificate for electronic signature/seal can terminate the validity of this certificate.

3.7 IDENTIFICATION AND VERIFICATION OF THE IDENTITY FOR THE RENEWAL OF A QUALIFIED CERTIFICATE*

** The procedure for renewing a qualified certificate is described in the Practice of Qualified Certification Services.*

3.8 IDENTIFICATION AND VERIFICATION OF IDENTITY IN THE EVENT OF SUSPENSION OF THE VALIDITY OF A QUALIFIED CERTIFICATE*

** The procedure for renewing a qualified certificate is described in the Practice of Qualified Certification Services.*

3.9 IDENTIFICATION AND VERIFICATION OF IDENTITY WHEN TERMINATING THE VALIDITY OF A QUALIFIED CERTIFICATE

When Evrotrust, trough the Registration Authority or on its own, terminates the validity of a qualified certificate, it records this in the databases with qualified certificates it maintains and publishes the cancelled status of the certificate in a timely manner, no later than 24 hours after the receipt of the request. The cancellation becomes valid immediately after its publication.

In the event of termination through Evrotrust's mobile application, no identity check will be carried out, having in mind the access of the Signatory to the respective functionality.

3.10 IDENTIFICATION AND VERIFICATION OF IDENTITY AFTER TERMINATING THE VALIDITY OF A QUALIFIED CERTIFICATE

The policy and practice of Evrotrust for providing qualified certification services do not allow renewal of a qualified certificate after it has been terminated.

The Signatory/Creator of a terminated qualified certificate can request a new certificate to be issued.

Evrotrust, through the Registration Authority, carries out initial identification and verification of the identity of the Signatory/Creator, if he requests a new certificate. Such a verification will not be carried out, if the user has requested the issuance of a new qualified certificate from the mobile application in which he has an active profile.

4 OPERATIVE REQUIREMENTS*

Through the Registration Authority, Evrotrust provides the following operating procedures for Qualified Certification Services in accordance with ETSI EN 319 411-1 and applicable to Qualified Electronic signatures/seals:

- registration of a request to issue a qualified certificate;
- processing of a request to issue a qualified certification;
- issuance of a qualified certificate;
- handing to a User the issued qualified certificate;

- renewal of a qualified certificate;
- suspension/restoration of the validity of a qualified certificate;
- termination of a qualified certificate.

** Operational procedures for Qualified Certification Services are described in the Practice of Qualified Certification Services.*

4.1 USE OF QUALIFIED CERTIFICATES AND KEY PAIRS

4.1.1 BY USERS

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

- according to their purpose;
- only during their validity period;
- when the certificate has been suspended, the user should not use the private key, especially to create an electronic signature/seal.

The responsibility for using the private key will be borne by the Signatory.

4.1.2 BY RELYING PARTIES

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

- according to their purpose;
- only after verification of their status and verification of the electronic signature of the Certifying Authority which issued the certificate;
- until the cancellation of the validity of a given key;
- when the certificate has been suspended, the relying party should not accept the public key.

4.2 RENEWAL OF A QUALIFIED CERTIFICATE

A renewal of a qualified certificate means to replace a valid certificate with a new one,

without changing the information existing in it, except for a new serial number and a new validity period.

A renewal is performed only within the validity period of a valid certificate. It has to be preceded by the registration of a request for renewal in suitable format, accepted and approved by an operator in a Registration Authority, with authentication and correctness of the submitted request.

Renewals of a remotely issued certificate, through the mobile application, will not be allowed.

4.3 ISSUANCE OF A QUALIFIED CERTIFICATE WITH GENERATION OF A NEW PAIR OF KEYS (RE-KEY)

A new pair of keys will be generated by Evrotrust in the cases where an already registered user requests to generate for him a new pair of keys, or when a new user requests to generate a pair of keys. The generation of a new pair of keys is accompanied by the issuance of a new qualified certificate confirming the ownership of the newly created key pair.

** Operational procedures are described in the Practice of Qualified Certification Services.*

4.4 CHANGES IN QUALIFIED CERTIFICATES

A change in a qualified certificate means a change in the content of the data in an already issued and published qualified certificate for an electronic signature/seal. In the event of changes in the qualified certificate, it is obligatory to generate a new pair of keys.

The change will be treated in the same manner as the issuance of a new qualified certificate.

4.5 SUSPENSION AND TERMINATION OF QUALIFIED CERTIFICATES

The suspension and termination of the validity of a qualified certificate will carried out only during the validity period of the certificate. The suspension leads to temporary suspension of the

validity of the certificate. The termination leads to irrevocable termination of the validity of the certificate.

If a certificate was terminated after the initial activation, it will lose its validity from the moment of termination and its status cannot be restored under any circumstances.

If Evrotrust suspends or terminates a qualified certificate, it will register this change in its database with qualified certificates and publish the cancelled status of the certificate in a timely manner. The suspension or termination enter into force immediately after the certificate was published in the repository.

The services for the management of termination and suspension of the validity of a qualified certificate are available 24 hours a day, 7 days a week.

The suspension of certificates issued remotely through the Evrotrust mobile application will not be allowed.

4.5.1 CIRCUMSTANCES FOR TERMINATING A QUALIFIED CERTIFICATE

Evrotrust will terminate a qualified certificate issued by it when the following hypotheses are present:

- when the information recorded in the certificate has changed;
- when it is suspected that the private key tied to the public key contained in the certificate has been compromised;
- the user decides to terminate the contract with Evrotrust;
- death or placing under guardianship of the Signatory/Creator;
- termination of the representative powers of the Signatory with respect to the Creator;
- when the User does not meet the requirements of the adopted Certification Policy;
- if the Certification Authority terminates its activity;
- if the User owes unpaid fees for qualified certification services provided;
- when the reliability and security of the private key of the Certifying Authority have been violated;
- when a User who is an employee of an organization terminates his employment contract without returning the cryptographic card used on which the certificate and the respective private key are stored.

4.5.2 PROCEDURE FOR TERMINATION OF A QUALIFIED CERTIFICATE

4.5.2.1 PROCEDURE FOR TERMINATION OF A QUALIFIED CERTIFICATE OF AN END-USER*

The termination of the qualified certificate of an end-user is preceded by submitting a request for termination to the Registration Authority of Evrotrust.

** The operational procedure for terminating a qualified certificate is described in the Practice of Qualified Certification Services.*

When using a mobile application, it is assumed that there is a request for termination when the User has activated the respective functionality established in the application. In this case, the above procedures will not be applied.

A terminated certificate will not be subject to restoration or renewal.

4.5.3 GRACE PERIOD FOR THE TERMINATION OF A QUALIFIED CERTIFICATE

Before suspending the validity of a qualified certificate, Evrotrust, through its Registration Authority will stop the validity of the certificate for a grace period until the reasons for the suspension have been clarified, but for no longer than 72 hours.

Within this period, Evrotrust will process the request to terminate the qualified certificate.

A grace period is not allowed for remotely issued certificates. They are terminated immediately.

4.5.4 ONLINE VERIFICATION OF THE STATUS OF A CERTIFICATE

Evrotrust provides qualified services for verification of the status of the issued certificates in real time. This service is carried out on the ground of a Protocol for online verification of the status of a certificate (OCSP), described in RFC 2560. The use of OCSP allows obtaining information concerning the status of the certificates, without the need to verify in the List of

Suspended and Terminated Certificates (CRL).

The OCSP service generates a response based on a database. The OCSP response is valid for up to 7 days. In order to maintain the correct operation of the system, the OCSP answers are cached for a predefined time (usually no more than several hours).

The verification of the status of a certificate in real time according to a OCSP protocol can be carried out on the Internet, on the webpage of Evrotrust: https://www.evrotrust.com.

4.5.5 CIRCUMSTANCES FOR THE SUSPENSION OF A QUALIFIED CERTIFICATE

Evrotrust, through its operative Certifying Authority („Evrotrust RSA Operational CA"), will suspend the validity of a certificate under certain conditions.

Evrotrust undertakes immediate actions under the request to suspend a certificate.

For the time when the certificate is suspended, it is deemed to be invalid and all electronic signatures/seals verified with this certificate will be null.

4.5.6 PROCEDURE FOR TERMINATION AND RESTORATION OF A QUALIFIED CERTIFICATE*

A suspension of the validity of a qualified certificate is preceded by the registration of a request for suspension before the Registration Authority.

** The operational procedure for suspending and resuming a qualified certificate is described in the Practice of Qualified Certification Services.*

After the termination of a certificate, Evrotrust will immediately notify the Signatory/Creator of the suspended qualified certificate. The suspension and restoration of qualified certificates issued remotely, through the mobile application, is not allowed.

4.5.7 GRACE PERIOD FOR SUSPENSION OF A QUALIFIED CERTIFICATE

Evrotrust will suspend the validity of a qualified certificate for electronic signature/seal for

a grace period until clarification of the reasons for the suspension, but for no more than 72 hours.

Grace periods for the suspension of qualified certificates issued remotely through the mobile application will not be allowed.

4.5.8 RESTORATION OF THE VALIDITY OF A SUSPENDED CERTIFICATE

Evrotrust will restore the validity of a suspended certificate:

- when the ground for suspension has ceased to exist before expiry of the suspension period;
- by request of the Signatory, after clarifying the reasons for the requested suspension;

After the restoration of a certificate, it will be deemed valid.

4.6 VERIFICATION OF THE CURRENT STATUS OF A QUALIFIED CERTIFICATE

Information on the status of certificates issued by Evrotrust can be obtained in the List of Suspended and Terminated Certificates (CRL) published on Evrotrust's website, and through the Protocol for Online Verification of the Status of the Certificates (OCSP).

The certification services for verification of the status of qualified certificates are accessible 24/7/365 (continuously operating).

4.7 TERMINATION OF A CONTRACT FOR QUALIFIED CERTIFICATION SERVICES BY A USER

The contract for qualified certification services between Evrotrust and a User will be terminated:

- upon expiry of the validity period of the last issued qualified certificate, if the user has not taken action to update his qualified certificate;
- when the qualified certificate has been terminated and the user has not taken action for the issuance of another certificate;
- upon cancellation of a User profile from the mobile application of Evrotrust. In this case, all issued qualified certificates will be terminated.

5 CONTROL OF PHYSICAL AND ORGANIZATIONAL SECURITY

5.1 CONTROL OF PHYSICAL SECURITY*

The measures taken in regards to the physical protection of Evrotrust are an element of the Information Security System, developed and implemented in Evrotrust which complies with the requirements of ISO 9001, ISO 22301, ISO/IEC 27001 and ISO/IEC 20000-1.

**The measures related to the physical protection of information data, technological systems, premises and related support systems are described in the Practice of Qualified Certification Services.*

5.1.1 PREMISES AND PREMISES STRUCTURE

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

5.1.2 PHYSICAL ACCESS

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

** The physical security of the systems is described in the Practice of Qualified Certification Services.*

5.1.3 STORAGE OF DATA CARRIERS

All carriers containing software, data archives, or audit information are stored in a strong-box in a special archive room with access control. There is a system of physical and logical protection in the premise of Evrotrust's archive.

5.1.4 DISPOSAL OF WASTE

Paper and electronic carrier containing potentially significant security information of Evrotrust shall be destroyed in special cutting devices after the expiry of the storage period specified in the internal rules.

Cryptographic keys information carriers and PIN/PUK codes used for their storage are fragmented by appropriate devices. This applies to carriers that do not allow permanent deletion of stored data and its reuse.

In certain cases, information from portable carriers is destroyed by deleting or formatting the device without an option for recovery.

5.2 ORGANIZATIONAL CONTROL

All security procedures for issuance, administration and use of qualified certificates for qualified electronic signature/seal are performed by trusted staff of Evrotrust.

Evrotrust maintains a sufficient number of qualified employees who ensure compliance with the applicable legislation and the company's internal rules and regulations at any time of its business.

5.2.1 TRUSTED ROLES

A detailed breakdown of staff functions and responsibilities is set out in the Evrotrust internal documents: job descriptions, permanent positions list and corresponding internal operational procedures.

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

5.2.2 REQUIREMENTS FOR SEPARATION OF RESPONSIBILITIES

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

5.3 STAFF CONTROL

Evrotrust staff consists of a sufficient number of highly qualified employees. Trusted persons possess 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 the 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 TRAINING REQUIREMENTS FOR EVROTRUST STAFF

The staff who performs functions and tasks arising from their employment at Evrotrust or employment at the Registration Authority (with the presence of an external Registration Authority) shall attend the following training courses:

- „On-the-job training in providing qualified certification services" by Evrotrust Technologies AD;
- „Policy for providing qualified certificate for qualified electronic signature/seal" by Evrotrust Technologies AD;
- orders, procedures and documentation related to the role taken;
- security technologies and security procedures used by the Certifying Authority and the Registration Authority;
- system software of the Certifying Authority and the Registration Authority;
- responsibilities arising from roles and tasks performed in the system;
- procedures performed in the event of the system failure or interruption of the activities of the Certification Authority.

5.4 EVENTS RECORDING AND MAINTENANCE OF JOURNALS

For the efficient management and operation of Evrotrust, all events having a significant impact on the security and reliability of the technology system, staff and users control and the

security impact of the qualified certification services provided are recorded.

Electronic journal information is generated automatically.

Journals of records for 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 Evrotrust authorized employee. After this period, the records are stored in archives.

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

5.4.1 VULNERABILITY AND ASSESSMENT

Evrotrust classifies and maintains registers of all assets in conformity to ISO/IEC 27001. According to the "Security Policy" of Evrotrust, an analysis of the vulnerability assessment of all internal procedures, applications and information systems is carried out. Analytical requirements may also be determined by an external institution authorized to perform an audit at Evrotrust.

The risk analysis shall be carried out at least once a year. The decision for proceeding with analysis is performed by the Board of Directors.

5.5 ARCHIVING

Information for significant events is archived in electronic form periodically.

Evrotrust archives all data and files related to: registration information; with system security; all requests submitted by users; all users' 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 archiving.

5.6 EVROTRUST ACTIVITY TERMINATION

5.6.1 REQUIREMENTS RELATED TO TRANSITION TO THE TERMINATION OF PROVIDER ACTIVITY

Before terminating its services, Certifying authority is required to:

- notify the Supervision Authority of its intention to terminate its services in the event of an action for declaring the company bankrupt, declaring the company invalid or of other request for termination or initiating winding-up proceedings. The notification shall be made 4 (four) months before the agreed date of termination;
- notify (at least 4 months before) its users for the decision to terminate the services it provides;
- changes in the status of its certificates;
- terminate all certificates of the users within the announced period for termination of the activity;
- inform all its users for the services termination;
- makes reasonable commercial efforts to minimize breaching of users' interests;
- pays compensation to users (compensation shall be proportional to the remaining period of the certificates validity);
- carry out the required actions in order the Supervision Authority to maintain Certificate Revocation List (CRL).

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

- inform Evrotrust about its intention to terminate the registration activity. The notification shall 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.
- The information under Art. Article 24 (2) (h) of Regulation (EU) No 910/2014 (all relevant information relating to data issued and received by Evrotrust, in particular with a view to providing evidence in court proceedings and ensuring continuity when providing the service) is stored for a period of 10 years, including after the termination of the activity of Evrotrust.

5.6.2 ACTIVITY TRANSFER TO OTHER PROVIDER OF QUALIFIED CERTIFICATION SERVICES

In order to ensure uninterruptedness of the qualified authentication services issuance to users, Evrotrust may sign an agreement with other 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 handing over of the activity;
- makes every effort and care to continue the issued user certificates validity;
- notify the Supervision Authority and the Users in writing that its activity is being undertaken by another registered provider as well as to give its name. The notification is published on the Evrotrust webpage;
- inform Users about the conditions of maintenance of the transferred certificates to the receiving Provider;
- change the status of the operating certificates and duly hand over all documentation related to its activity to the receiving Provider, together with all the archives and all issued certificates (valid, suspended and terminated);
- carry out the necessary actions for the transfer of 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 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 shall be delivered to the Provider accepting the activity.

5.6.3 WITHDRAWAL OF A QUALIFIED PROVIDER'S STATUS OR A QUALIFIED STATUS OF A RELEVANT SERVICE

In the event of withdrawal of the qualified Evrotrust status or of any of its certification services, provided by it, it shall carry out the following:

- informs its users about the changed status 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 commercial reasonable efforts to minimize consumer interests' violation.

6 TECHNICAL SECURITY MANAGEMENT AND CONTROL

6.1 GENERATING AND INSTALLATION OF A KEY PAIR OF THE CERTIFYING AUTHORITY

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

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

- to sign the operating certificates issued to the Certification Authorities in its infrastructure;
- to sign issued and published Certificate Revocation List (CRL);
- to sign all issued and published qualified certificates for electronic signatures/stamp of the Users.

6.1.1 GENERATING OF A KEY PAIR OF SIGNATORY/CREATOR

The key pair of Signatory/Creator of a certificate for qualified electronic signature/stamp is generated only on Secure Signature Creation Device (QSCD) approved by Evrotrust and verified for security and successful operation through Evrotrust infrastructure interfaces.

When the key pair is generated at Evrotrust, Secure Signature Creation Device (QSCD) (QSCD) is always used. The generated key pair private key cannot be taken off the device.

The private key control is through an access code. The Signatory uses the private key to create a signature/stamp by entering the access code at the Secure Signature Creation Device (QSCD).

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

In cases where the key pair is generated by Signatory/Creator, the latter shall bear full responsibility for the protection of the private key in order to prevent its compromising, disclosure, modification, loss or unauthorized use.

The Signatory/Creator bears responsibility for omissions or actions of the authorized persons who are authorized to generate, keep, or store their private keys.

The Signatory/Creator undertakes to use licensed software to operate a Secure Signature Creation Device (QSCD).

6.1.1.1 REQUIREMENTS TO SECURE SIGNATURE CREATION DEVICE (QSCD)

Secure Signature Creation Devices (QSCDs) guarantee by appropriate technical and procedural means, at least that:

- the confidentiality of electronic signature/stamp creation data used for creating the electronic signature/stamp is reasonably guaranteed;
- the data for creating an electronic signature/stamp are found only once in practice;
- the data for creating an electronic signature/stamp are sufficiently secured and cannot be retrieved, and the electronic signature/stamp is reliably protected against falsification, using the technology currently available;
- the data for creating an electronic signature/stamp can be reliably protected by the legitimate Signatory/Creator of the electronic signature/stamp against use by others.

Secure Signature Creation Devices do not alter the data to be signed and do not impede their submission to the Signatory/Creator of the electronic signature/stamp before signing.

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

6.1.1.2 REMOTE GENERATING OF PAIR KEYS

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

Private key generating, use and storage has a very high level of security that is guaranteed by the carrier itself. It is reliably protected by a Personal Identification Number (PIN) known only to the Signatory/Creator or an authorized representative of the legal entity.

The Signatory/Creator or the 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 format contains DN, public key and other attributes, all of which are signed by the private key.

In the event of remote generating of the key pair when issuance of certificate by the Evrotrust mobile application is applied for, it is generated in a Evrotrust hardware crypto module that complies with the requirements of the Regulation for Secure Signature Creation Device.

6.1.1.3 DELIVERY/ACCEPTANCE 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 on a secure signature creation device (QSCD) at the Registration Authority of the Provider.

The Initial User and Administrative Code for accessing and unblocking of the device is provided to the Signatory/Creator or the authorized representative of the legal entity in a sealed, opaque paper envelope.

The Signatory/Creator or the authorized representative of the legal entity is required to change its initial User Access Code to the device using the software provided with it. Evrotrust recommends that the Signatory/Creator or the authorized representative of the legal entity periodically changes its User Code.

In the event of remote generating of the key pair, the private key is generated and stored in an encrypted form in the Evrotrust hardware crypto module. The key encryption is created by a PIN-code of the Signatory/Creator, which ensures that only he has the permission to activate the key.

6.1.2 SUPPLY OF A PUBLIC KEY BY PROVIDER'S USER

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

The Signatory/Creator or the authorized representative of the legal entity delivers the public key of the generated key pair via an electronic key form, which format is PKCS # 10 through the Evrotrust Registration Authority. The request contains public key and is signed electronically

by the corresponding private key.

The user may provide an electronic request on a carrier, personally to the Registration Authority, together with the other documents in conformity to the Evrotrust Policy or via the Evrotrust web page.

The registration authority of Evrotrust shall 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 for through the Evrotrust mobile application.

6.1.3 KEY LENGTH

The length of a pair key of qualified electronic signature/stamp of User generated through the Evrotrust infrastructure is 2048 bits, with a combination of asymmetric and hash algorithms: sha256-with-RSA.

Regardless of where the pair key for the certificate of qualified electronic signature/stamp is generated, the key shall have a length of at least 1024 bits for RSA and DSA algorithms and 160 bits for ECDSA algorithms.

6.1.4 PUBLIC KEY PARAMETERS

The Signatory/Creator or the authorized representative of the legal entity of a pair key 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 to create an electronic signature and perform a check.

Secure signature creation devices (QSCD) and the provided environment for generating and storing the Signatory's/Author's or the authorized representative's keys are CC EAL 4+ and FIPS 140-2 Level 3 Security Levels.

All Secure signature creation devices (QSCD) that are outside the Evrotrust infrastructure that users can use to generate a key pair and store the private signature/stamp key shall be certified to Security level CC level EAL 4+ and a higher equivalent level.

6.1.5 USING A CRYPTOGRAPHIC ALGORITHM

When the cryptographic pair of keys (private and public) of the issued electronic signature / seal certificates is generated by the Holder / Creator, the user complies with the following requirements:

- Hash algorithms and asymmetric algorithms that meet the requirements of ETSI TS 119 312 are used to generate the keys;
- the applicable combinations of asymmetric and hash algorithms over the security of the qualified electronic signature over time is as specified in ETSI TS 119 312;
- The length of the key that meets the requirements of ETSI TS 119 312 is used.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPH MODULE CONTROL

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

6.2.1 CONTROL OF PERSONAL KEY USE AND STORAGE

The private key of the Signatory/Creator or the authorized representative of the legal entity is only used in secure signature creation devices (QSCD) or a device with an equivalent level of security (as required by Regulation (EU) No 910/2014) and is accessible through a personal access code. Simultaneously with generating a pair key of the Signatory/Creator or the authorized representative of the legal entity, private key storage is performed in a secure signature creation device (QSCD).

Evrotrust does not in any way store or archive a private key of a User for creating an electronic signature/stamp, except in the case of remote request of a qualified certificate through the Evrotrust mobile application. In this case, the private key is generated and stored in encrypted form in the Evrotrust hardware crypto module. The key encryption is a PIN-code created by the Signatory/Creator that ensures that only he has the permission to activate the key.

6.2.2 PERSONAL KEY STORAGE

Evrotrust does not create copies of users' private keys except in the case of the previous paragraph. The private key of the Signatory/Creator or the authorized representative of the legal entity is only stored on secure signature creation device (QSCD) and cannot be reproduced on another device. Upon defecting of the secure signature creation device (QSCD), the User shall replace it and request the issuance of a new qualified certificate.

6.2.3 METHOD FOR PERSONAL KEY ACTIVATION

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

6.2.4 METHOD FOR PERSONAL KEY DEACTIVATION

The private key of the Signatory/Creator or the authorized representative of the legal entity is deactivated by terminating the logical access to the secure signature creation device (QSCD), or by physical destruction. This will permanently disable the private key access and use.

6.2.5 METHOD FOR PERSONAL KEY DESTROYING

The private key of a qualified user certificate is destroyed by its deleting by the secure signature creation device (QSCD) or by the device physically destroying.

6.3 OTHER ASPECTS OF KEY PAIR CONTROL

6.3.1 PUBLIC KEY ARCHIVING

Public Keys of the Signatory/Creator or the authorized representative of the legal entity are contained in the qualified certificates issued to them, which are published in the Register of

issued certificates of the Evrotrust website and stored in a repository.

6.3.2 QUALIFIED CERTIFICATE PERIOD OF VALIDITY AND KEYS USE

The period of public keys use is determined by the value of the field in its certificate describing the public key validity. Evrotrust issues qualified certificates with a validity period of 1, 2 or 3 years. The validity of the certificates and their respective private keys may be cut down in the event of the certificates termination.

6.4 ACTIVATION DATA

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

In cases where the Signatory/Creator or the authorized representative of the legal entity generates a key pair for qualified certificate, they create and control the activation data themselves.

6.4.1 ACTIVATION DATA GENERATING AND INSTALLATION

Activation data are used at the initial issue of a certificate on a secure signature creation device (QSCD) before generating a key pair. 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.

Codes for access and unblocking of a secure signature creation device (QSCD) are provided to the Signatory/Creator or the authorized representative of the legal entity in a sealed, opaque paper envelope.

The Signatory/Creator or the authorized representative of the legal entity is required to change the initial User Access Code using the software provided together with the device.

Evrotrust recommends that the Signatory/Creator or the authorized representative of the legal entity periodically to change its User Access Code to the secure signature creation device

(QSCD).

The user shall use the provided Administrative Access Code to unblock a blocked device.

When using a mobile application of Evrotrust, the access code is generated by the Signatory/Author. 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 answers to three secret questions asked by the user at the time of registration via the mobile application. The answers to the questions are not kept by Evrotrust.

6.4.2 ACTIVATION DATA PROTECTION

The Signatory/Creator or the authorized representative of the legal entity is required to store and protect against compromising access codes to secure signature creation device (QSCD).

Users need to know that after a few unsuccessful attempts to access the device; they are blocked (locked). In these cases, the user shall use the Administrative Access Code provided to unblock the device.

Evrotrust recommends that device activation data never to be stored together with the device itself.

6.5 COMPUTER SYSTEMS SECURITY

Evrotrust uses only 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 for local access protection to software and information data.

Evrotrust uses procedures for information security control of the entire Evrotrust infrastructure in conformity to the international practice standards generally adopted.

6.6 TECHNOLOGY SYSTEM LIFE CYCLE SECURITY

All hardware changes are monitored and registered by authorized Evrotrust employees. The new technical equipment purchase is supplied with the necessary operating procedures and instructions for use.

Supervision of the technological system functionality is implemented and it ensures that it functions properly and is delivered in conformity to manufacturing configuration procedures.

6.7 NETWORK SECURITY

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

7 QUALIFIED CERTIFICATES PROFILES FOR QUALIFIED ELECTRONIC SIGNATURES/STAMPS

User qualified certificates profiles conform to the format described in standard ITU-T X.509 v.3. certificate of the type X.509 v.3 is a dataset that uniquely authenticates the belonging of the public key to the creator of the qualified electronic signature/stamp.

8 PROVIDER'S ACTIVITY VERIFICATION AND CONTROL

Verifications (audits), carried out at Evrotrust refer to processing of information data and management of key procedures.

Evrotrust annually performs one internal audit at least.

Evrotrust is performing audit every three years according to ISO / IEC 27001: 2013, ISO 9001: 2015, ISO 22301: 2012 and ISO / IEC 20000-1:2011 and annual partial audits of these standards.

Evrotrust is audited at least once every 24 months by a Conformity Assessment Body. The purpose of the audit is to confirm that the Qualified Certification Services Provider and the provided qualified certification services meet 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 Conformity Assessment Body shall be transmitted to the Supervisory Authority within 3 (three) days of its transmission to Evrotrust management. The Supervisory Authority examines the report and decides whether to leave or take the qualified status of Evrotrust.

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

Evrotrust staff undertakes specific actions for their remedy within the specified deadlines.

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 PRICES AND FEES

Evrotrust maintains a document "Pricing for certification, information, cryptographic and advisory services" on its webpage: https://www.evrotrust.com/blanki/tarifa.pdf.

9.1.1 CERTIFICATE RETURN AND RECOVERY OF PAYMENT

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

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

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

The User may refuse the issued qualified certificate with true content that Evrotrust will terminate immediately without recovering the payment for the revoked certificate.

9.2 FINANCIAL RESPONSIBILITY

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

Evrotrust shall bear responsibility if the damage is through his fault or through the fault of the persons to whom he has assigned the job.

If Evrotrust confirms and accepts that damages have occurred, it undertakes to pay the costs of damages fixing. The maximum payment limit may not exceed the amount of the damages.

9.2.1 INSURANCE OF ACTIVITY

Evrotrust undertakes compulsory insurance of its activity as a registered Provider of qualified certification services.

9.3 INVIOLABILITY OF PERSONAL DATA

Evrotrust is registered as Personal Data Administrator 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 the Signatories/Creators or the 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 are subject to intellectual property rights and other material and non-material rights.

9.4.1 RIGHT OF OWNERSHIP OF A KEY PAIR

The users' key pair and the associated public key certificate issued by Evrotrust, as well as the relevant secret material, are ownership of Evrotrust, regardless of the ownership of the physical environment where the keys are stored and protected.

9.5 LIABILITIES, RESPONSIBILITY AND GUARANTEES OF EVROTRUST

Evrotrust ensures that it implements its activities as:

- strictly adheres to the terms of this document, the requirements of Regulation (EU) No 910/2014 and the national legislation in the implementation of its activity as a Qualified Certification Services Provider;
- the services provided do not infringe third parties copyright and licensed rights;
- uses technical equipment and technologies to ensure system reliability and technical and cryptographic security in the processes implementation, including a secure and secure mechanism/device for generating keys and for creating a qualified electronic signature/stamp in its infrastructure;
- issues qualified certificates for electronic signatures/stamps after verifying the presented information by lawful means;
- securely store and maintain information related to the issued certificates and the systems operation;
- complies with established procedures for work and rules for technical and physical control, in accordance with the terms of this Policy and "Practice in the provision of Qualified Certification Services";
- creates an opportunity for immediate suspension and termination of a qualified certificate;
- terminates and suspend certificates operation under the terms and conditions of the relevant Policy;
- notifies stakeholders immediately after the qualified certificate suspension;
- provides conditions for accurate defining the time of issue, suspension, renewal and

termination of qualified certificates;

- performs procedures for identification and authentication of the Signatory/Creator or of the authorized representative of a legal person;
- ensures measures against counterfeiting of qualified certificates and data confidentiality to which an access is provided in the process of creating the qualified electronic signature/stamp;
- uses reliable systems for certificates storing and management;
- only duly authorized employees have access to make changes in data, establish the certificates authenticity and validity;
- takes immediate measures in the event of technical security issues;
- upon the expiration of the validity period of a qualified certificate, it shall revoke its validity;
- inform the Signatories/Creators or the authorized representatives of legal entities as well as the relying parties on their obligations and due diligence on the use and trust of the qualified certification services provided by Evrotrust as well as on the correct and safe use of the qualified certificates issued and the provided certification services relating thereto;
- use and store the collected personal and other information only for the purposes of its activity in providing qualified certification services in accordance with national law;
- does not store or copy data for creation of user's private keys, except for remote requesting of qualified certificates through the Evrotrust mobile application;
- maintains disposable funds that enable it to carry out its activities;
- concludes insurance for the time of its activity;
- maintains trusted staff, possessing the required level of knowledge, experience and qualification to carry out the activity;
- maintains Repository where it publishes the qualified certificates issued, the current Certificate Revocation List (CRL), other circumstances and electronic documents pursuant to this Policy and the National Legislation;
- provides permanent access to the Register of certificates by electronic means (24/7/365);
- provides protection against making changes to the Repository maintained by unauthorized or unauthorized access or due to accidental occurrence;

- immediately publish in the Register of certificates the certificates issued and signed;
- creates conditions for each relying party to verify the status of the issued and published qualified certificate in the Register of Certificates;
- perform periodic internal audits of the activity of the Certifying Authority and the Registration Authority;
- perform external audits by independent auditors and publish the results of the audit on its website;
- use certified software and hardware as well as secure and reliable technological systems in its activity;
- maintains a list of Registration Authorities, a list of recommended software and user hardware, forms, templates, standard contract, etc. documents of help for the users on the Evrotrust website;

Evrotrust shall bear responsibility to Users and Relying Parties for damages caused by gross negligence or intent:

- of failure to comply with the requirements of Regulation (EU) No 910/2014 in carrying out its activity of providing qualified certification services;
- of incorrect or missing data in the qualified certificate at the moment of its issuance;
- of damages caused if, during the issuance of the qualified certificate, the person named as Signatory/Creator or authorized representative of a legal entity have not have the private key corresponding to the public key;
- of algorithmic discrepancy between the private key and the public key entered in the qualified certificate;
- of failure to comply with the obligations to issue and manage qualified certificates
- of omissions in establishing the identity of the Signatory/Creator or the authorized representative of a legal entity.

9.5.1 LIABILITIES, RESPONSIBILITY 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, 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 ensures that the Registration Authority:

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

9.6 USERS OBLIGATIONS

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

- to become acquainted with and comply with the conditions of the Contract, Policies and Practices in the provision of qualified certification services by Evrotrust, as well as the requirements in the other documents published on the website of Evrotrust;
- when requesting the issue and management of qualified certificates to provide true, accurate and complete information which is required pursuant to the Contract, the legal requirements, the applicable Policies and Practices by Evrotrust;
- generate cryptographic keys using a secure method and algorithm in accordance with the requirements of Regulation (EU) No 910/2014 and use QSCD devices, approved by Evrotrust;
- verify the completeness and veracity of the content of the authentication information provided by it in the Distinguished Name (DN) field of the issued qualified certificates. In the event of a discrepancy between the submitted information and the certified content, the user shall

immediately notify Evrotrust;

- discontinue the use of a qualified certificate in case of a doubt about loss or compromising of the private key and to submit a request for its suspension to Evrotrust;
- to discontinue the use of a qualified certificate in the presence of old, altered, incorrect and / or false information in it and to file a request for suspension of the certificate operation;
- before using a new qualified certificate, to change the current PIN for access to the secure signature creation device (QSCD) where the private key is stored;
- to apply due diligence and take appropriate measures to prevent the private key from compromising, losing, disclosing, modifying or otherwise unauthorized access;
- use the qualified certificate issued by Evrotrust only for lawful purposes and in accordance with the policy and practice specified therein;
- approve the terms and conditions set out in the Agreement between him/her and Evrotrust (this approval is in the form of a handwritten signature on the agreement);
- approve the qualified certificate issued to him/ her;
- not to disclose the password for access to the secure signature/stamp creation device to unauthorized persons;
- not to make your private key available to others.

9.7 DISCLAIMER

Evrotrust is not responsible for any damages caused by:

- the use of a qualified certificate outside the limits of the assigned functions and limitations of its validity;
- Illegal actions of Users and Relying Parties;
- providing the means of identifying the device for creating a qualified electronic signature /stamp and access to the private key by Users of third parties;
- incidental events of force majeure, including malicious acts of third parties (hacker attacks, suspension of a secure signature creation device (QSCD), access to the private key, getting to know the way of Identification, without the Signatory's/Creator's knowledge of etc.);
- use of a qualified certificate that is not 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);
- no timely action for termination or suspension of a certificate (due to a request delayed by the Signatory/Creator or for reasons beyond Evrotrust's control);
- 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 the Signatory/Creator and Relying Parties.

Evrotrust is not responsible for using the certificate beyond the limits of the transaction value limits and usage objectives.

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 RESPONSIBILITY OF THE SIGNATORY/CREATOR

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 the authorized representative of a legal entity is liable to Evrotrust and to the Relying Parties if:

- In creating the private-public key pair, it has used an algorithm and secure signature creation device (QSCD) that do not meet the requirements of Regulation (EU) No 910/2014;
- does not exactly meet the security requirements set by Evrotrust;
- does not ask Evrotrust to suspend or terminate the validity of a qualified certificate after getting to know that the private key has been used improperly or there is a risk of its unlawful use;
- has made false statements made to Evrotrust concerning the content or issuance of the qualified certificate;
- when the qualified certificate is issued by a registered Creator and a person authorized by him (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.

9.9 GENERAL CONDITIONS

Evrotrust applies the requirements set out in ETSI EN 319 411-1, clause 6.9.4.

In addition, Evrotrust applies the following specific requirements:

- The policy is intended for issuing and providing qualified certificates and requires the use of QSCD;
- Supports a public key infrastructure statement;
- The statement on public key infrastructure is structured in accordance with Annex A of ETSI EN 319 411-1.

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.