QUALIFIED REGISTERED ELECTRONIC MAIL SERVICE

POLICY AND PRACTICE

CONTENTS

1 INTRODUCTION

"Evrotrust Technologies" AD (Evrotrust) is a qualified trust service provider exercising activity in accordance with the requirements of 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 the Electronic Document and Electronic Trust Services Act (ZEDEUU) and as such, the company is registered in the trust list of the European trust service providers (https://webgate.ec.europa.eu/tl-browser/#/tl/BG), as well as in the register of Bulgarian trust service providers maintained by the Communications Regulation Commission (CRC) (http://crc.bg/files/_bg/Register_site_bg_30092017_Last_LAST.pdf).

Evrotrust provides to its users highly reliable and secure qualified registered electronic mail service in accordance with Art. 44 of Regulation (EU) No. 910/2014.

1.1 OVERVIEW

„The Qualified Registered Electronic Mail Service Policy and Practice (the Policy and Practice) is a document that describes the general rules and regulations applied by "Evrotrust Technologies" AD (Evrotrust) in the provision of the qualified registered electronic mail service (QREMS). This document applies to a trust service provided by Evrotrust in line with Art. 44 of Regulation (EU) No. 910/2014 and in line with the applicable legislation in Republic of Bulgaria.

The Electronic Registered Delivery Service (ERDS) provides secure and reliable delivery of electronic mails between the parties and offers evidence for the delivery process. The evidence can be considered statements by a trusted party, more specifically – Evrotrust, that a certain event related to the delivery process (sending, forwarding, transmission, message denial, etc.) happens at a specific moment. The evidence can be transmitted immediately (together with the message or separately) or it can be stored in Evrotrust's storage for later access. Evrotrust creates evidence in the form of digitally signed data.

The Qualified Electronic Registered Delivery Service (QERDS) policy and practice contains the main terms and requirements that also apply to the QREMS Policy and practice. This document makes references to the relevant provisions and specific requirements described in the QERDS Policy and practice and contains the additional requirements that apply solely to

QREMS.

Regulation (EU) No. 910/2014 provides the legal framework for facilitation of cross-border cooperation in the European Union (EU) for recognition of the existing national law systems related to the registered electronic mail service. The ERDS standards framework aims to cover the general and globally recognised requirements for registered electronic mail provided in a secure and reliable manner, irrespective of the applicable legislation.

This document defines the common requirements towards the activity of Evrotrust in its capacity as a qualified registered electronic mail service provider (QREMSP). This policy sets out the provisions that apply to company staff (competences, responsibilities, authorisation and obligations based on the role of each employee).

QREMS is a specific type of registered electronic mail that is based on the formats, protocols and mechanisms used in normal e-mail messages. Evrotrust, as a provider of this service, meets a certain number of additional requirements set out in this document. The QREMS standards framework aims to cover the general and globally recognised requirements for secure and reliable registered electronic mail.

Evrotrust performs secure initial identification of the recipient and the sender and protection against loss, theft, corruption or unauthorised change of the data transmitted, thus ensuring the integrity of the user content.

It is extremely important for Evrotrust users to familiarise themselves with the objectives and the role of this Policy and practice so that this service can be put into practice.

The relationships between Evrotrust and the users shall be settled through a Contract.

This document is in line with the standard ETSI EN 319 531 Electronic Signatures and Infrastructures (ESI) Policy and security requirements for Registered Electronic Mail Service Providers.

This policy is a public document. It can be changed at any time by Evrotrust and each new revision shall be approved by the Board of Directors and communicated to all relevant stakeholders through the company website (https://www.evrotrust.com).

1.1.1 LEGISLATIVE REFERENCES

This policy and practice is in line with the following legal documents, standards and

recommendations:

- 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;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements;
- ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps;
- ETSI EN 319 522-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 1 Framework and Architecture;
- ETSI EN 319 522-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 2 Semantic Contents;
- ETSI EN 319 522-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 3: Formats;
- ETSI EN 319 522-4-1 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-1 Message delivery bindings;
- ETSI EN 319 522-4-2 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-2 Evidence and identification bindings;
- ETSI EN 319 522-4-3 Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services Part 4-3 Capability and requirements bindings;
- EN 319 532 Part 1 Registered Electronic Mail (REM) Services. Framework and Architecture;
- EN 319 532 Part 2 Registered Electronic Mail (REM) Services. Semantic Contents;
- EN 319 532 Part 3 Registered Electronic Mail (REM) Services. Formats;
- EN 319 532 Part 4 Registered Electronic Mail (REM) Services. Interoperability profiles;
- ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers;
- ETSI EN 319 531 Electronic Signatures and Infrastructures (ESI) Policy and security

requirements for Registered Electronic Mail Service Providers;

1.2 DOCUMENT NAME AND IDENTIFIER

The full name of this document is "Qualified Registered Electronic Mail Service Policy" of Evrotrust Technologies AD and an identifier:

Policy name	Object Identifier (OID)
QUALIFIED REGISTERED ELECTRONIC MAIL SERVICE POLICY AND PRACTICE	1.3.6.1.4.1.47272.2.10.2

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.

1.3 PARTICIPANTS IN THE INFRASTRUCTURE

1.3.1 REGISTRATION AUTHORITY

The description of the registration authority is in the document entitled "Qualified Electronic Registered Delivery Service Policy" of "Evrotrust Technologies" AD.

1.3.2 USERS

The description of the user is in the document entitled "Qualified Electronic Registered Delivery Service Policy" of "Evrotrust Technologies" AD.

1.3.3 RELYING PARTIES

The description of the relying parties is in the document entitled "Qualified Electronic Registered Delivery Service Policy" of "Evrotrust Technologies" AD.

1.3.4 OTHER PARTICIPANTS

The description of other participants is in the document entitled "Qualified Electronic Registered Delivery Service Policy" of "Evrotrust Technologies" AD.

1.4 APPLICATION OF ELECTRONIC RECOMMENDED POST

Registered electronic mail (REM) is a specific type of registered electronic mail that is based on the formats, protocols and mechanisms used in normal e-mail messages. Regulation (EU) No. 910/2014 defines a qualified electronic registered delivery service (QERDS), which is a specific type of ERDS and where the service and its provider shall meet a certain number of additional requirements.

The qualified registered electronic mail service (QREMS) allows sending and/or receiving of a consignment that contains user content (e.g. electronic documents) related to it or to its transport metadata and REMS evidence for this process. This service is a useful tool for rapid and reliable delivery of information. Evrotrust ensures the security and safety of the communication with authentication of the time when the user content has been sent by the sender and authentication of the time of receipt of the user content by the recipient, as well as evidence for the communication that guarantees the authenticity of the exchanged deliveries. The evidence can be transmitted immediately (together with the user content or separately) or it can be stored in Evrotrust's storage for later access.

The service is designed both for individuals and legal entities, for administrations, public figures and organisations providing public services.

1.5 MANAGEMENT OF POLICY AND PRACTICE

1.5.1 MANAGEMENT POLICY ORGANIZATION

Evrotrust is responsible for managing this Policy and practice. An organization has been set up to review the documents and make timely updates.

Any version of the Policy and Practice is in force until the approval and publication of a new version. Each new version is developed by Evrotrust employees and, after approval by the

Eurotrust Board of Directors, is published on the Evrotrust website: https://www.evrotrust.com/landing/en/a/tsp-documents.

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

1.5.2 CONTACT PERSON

The contact person in relation to the management of the "Qualified Registered Electronic Mail Service Policy of "Evrotrust Technologies" AD shall be the Chief Executive Officer of Evrotrust.

Further information can be requested at the following address:

Evrotrust Technologies AD

Sofia, 1766, Bulgaria

„Business center MM", floor 5, Bul. "Okolovrasten pat" 251G

Contact telephone: + 359 2 971 44 61 – information/registration authority/technical support

Website: http://www.evrotrust.com

E-mail address: info@evrotrust.com

1.6 DEFINITIONS AND ABBREVIATIONS

1.6.1 DEFINITIONS

Qualified Registered Electronic Mail Services Provider/QREMSP) – a qualified provider of qualified trust services that provides a registered electronic mail service in accordance with Regulation (EU) No. 910/2014;

Electronic Registered Delivery Service (ERDS) - an electronic service that allows electronic data transmission between a sender and a recipient and presents evidence related to the processing of the data transmitted, including evidence for sending and receiving the data, which also protects the data transmitted from the risk of loss, theft, damages or any unauthorised changes;

ERDS evidence - data generated by the registered electronic mail service the purpose of which is to prove that a given event has happened during a specific period of time;

ERDS handover metadata - data related to the user content generated by the registered

electronic mail and handed over to the recipient's agent/ERD;

ERDS notification/return receipt - an ERD message that contains evidence for ERDS and some metadata;

Delivery – an action where the sender's user content has successfully crossed the border with the user agent/application of the recipient;

REMS consignment - data structure that contains the user content, REMS metadata and/or REMS evidence;

REM handover metadata - data related to the user content generated by REMS and handed over to the user agent;

Registered Electronic Mail Service (REMS) - a service that allows electronic data transmission between entities, provides evidence related to the processing of the data transmitted, including evidence for the data sending and receiving, which also protects the data transmitted against the risk of loss, theft, corruption or unauthorised changes;

Qualified Registered Electronic Mail Service (QREMS) - registered electronic mail service that meets the requirements set out in Art. 44 of Regulation (EU) No. 910/2014;

REMS evidence - data generated as part of the registered electronic mail service, which have the purpose to prove that a certain event has taken place at a certain moment;

Store and Forward (S&F) - REMS operation style (REM Store and Forward) of Evrotrust, where the user content that has been created and sent by the sender is transmitted to the recipient without an express requirement for confirmation by the recipient; After the sender sends the content, the recipient is not required to perform any other action, except for identification and authentication. For this purpose, the user content shall be stored at the recipient's system.

User content - original data created by the sender that should be delivered to the recipient. It can consist of one or more files. The body of the e-mail message and all files attached, if any, constitute user content.

UA/User Agent - user agent/application. This is a system comprising of software and/or hardware components used by the sender/recipient to participate in the data exchange with the registered electronic mail service providers;

Recipient - an individual or a legal entity to whom user content is addressed;

Sender - an individual or a legal entity that provides user content;

Interface – in this case this term shall mean user interface, which constitutes a shared border between two separate computer components that exchange information which is used

for access to resources.

1.6.2 ABBREVIATIONS

EDETSA – Electronic Document and Electronic Trust Services Act;

QTSP – Qualified Trust Service Provider;

ERDS - Electronic Registered Delivery Service;

QERDS – Qualified Electronic Registered Delivery Service;

REM - Registered Electronic Mail;

REMS - Registered Electronic Mail Service;

QREMS - Qualified Registered Electronic Mail Service;

QERDSP – Qualified Electronic Registered Delivery Service Provider;

QREMSP - Qualified Registered Electronic Mail Service Provider;

UA (user agent) – user agent/application;

S&F - Store and Forward;

SMTP - Simple Mail Transfer Protocol - an internet standard for transfer of electronic mail;

IMAP - Internet Message Access Protocol;

TLS - Transport Layer Security – a cryptographic protocol that ensures the security of internet communication.

2 RESPONSIBILITY FOR PUBLICATION AND STORAGE

The public register is available at: https://www.evrotrust.com/.

Evrotrust publishes communication related to the company activity and all significant documents that might be of interest for the users and the relying parties at its website.

Users and relying parties shall be informed about the Policy, Practice and General Terms of the Registered Electronic Mail Service before signing a contract. The documentation, including Policy and Practice, agreements, models, audit reports, etc. is published on the Eurotrust website immediately on each update. The operational certificates of the certifying authority are published immediately upon each issue of new certificates.

Evrotrust offers services related to access to the information stored in the repository (the public register), providing HTTP / HTTPS based access to it. The information published in the Evrotrust

repository is permanently accessible (24/7/365), except in the cases of events beyond Eurotrust's control.

3 IDENTIFICATION AND CERTIFICATION OF IDENTITY

3.1 NAMES

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

3.2 INITIAL VERIFICATION OF IDENTITY

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

3.2.1 ESTABLISHING THE IDENTITY OF A NATURAL PERSON

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

3.2.2 ESTABLISHING THE IDENTITY OF A LEGAL PERSON

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

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

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

3.3 AUTHENTICATION

If a re-use request is required, in this case there is no initial identification, but only an authenticity / identity check. The user uses QREMS after being authenticated. Depending on the user agent / program (UA) used through which the sender and the recipient communicate with the electronic mail system, they are authenticated as follows:

1. If an e-mail client (eg Mozilla Thunderbird) is used, the authentication is done by using a pair of cryptographic keys with an attached certificate for advanced / qualified electronic signature / seal that are generated and issued in accordance with the Evrotrust policies and practices for the provision of qualified certificates for Qualified / Advanced Electronic Signature / Seal.
2. If a person uses a web interface to access e-mail, a pair of cryptographic keys with an attached certificate for advanced / qualified electronic signature / seal shall be used for authentication purposes generated and issued in accordance with the Evrotrust policies and practices for the provision of qualified certificates for Qualified / Advanced Electronic Signature / Seal.

Apart from the described ways of authentication, Evrotrust applies additional mechanisms in order to achieve maximum security and protection of the process.

4 SERVICE DELIVERY PROCESS

4.1 REQUIREMENTS TOWARD THE QUALIFIED REGISTERED ELECTRONIC MAIL SERVICE

QREMS allows transfer of user content between a sender and a recipient who are users of Evrotrust. This service provides evidence for the integrity and time of data transmission, including evidence for their sending and receipt. The service protects the data against loss, theft, breach of their integrity or unauthorised change and meets the requirements of QERDS in accordance with Regulation (EU) No. 910/2014.

The QREMS service provided by Evrotrust complies with the following requirements:

- Evrotrust guarantees the sender's identity;
- Evrotrust guarantees the recipient's identity before the delivery of data (the consignment/user content);

- sending and receipt of the user content is backed by evidence signed with an advanced electronic seal of Evrotrust in a way that precludes any possibility for any unnoticed change in the user content;
- any change in the data that is necessary for the purpose of sending or receiving the data is clearly marked both for the sender and the recipient of the data;
- the date and time of sending and receiving are noted with a qualified electronic time stamp;
- the availability, integrity and confidentiality of user content is guaranteed from the time of sending it until its receipt;
- the integrity of the user content is protected during the exchange between the sender and the recipient or among the distributed system components of the service;
- the sender predefines the period during which the QREMS system attempts to deliver the user content. If the sender does not select an option, the default period is 3 days;
- QREMS uses the qualified services of the QTSP "Evrotrust Technologies" AD for issue and management of qualified certificates (X.509) and qualified time stamps;
- the entire information on the provision of QREMS is stored for a period of 10 years in line with the national legislation of Republic of Bulgaria (EDETSA).

4.2 DESCRIPTION OF TECHNOLOGY

QREMS uses a technology, where, after the initial identification of the sender and its current authentication through the registered e-mail address in the qualified certificate for advanced electronic signature, the user content is accepted by S-REMS through a properly secured and encrypted channel. At this moment, S-REMS generates the necessary evidence with integrated data about the type of event, including date, time, control/hash sum of the user content, which are electronically signed by the Certifying Authority for QREMS and signed with a qualified time stamp. If S-REMS is unable to accept, the system automatically generates the necessary evidence for the refusal.

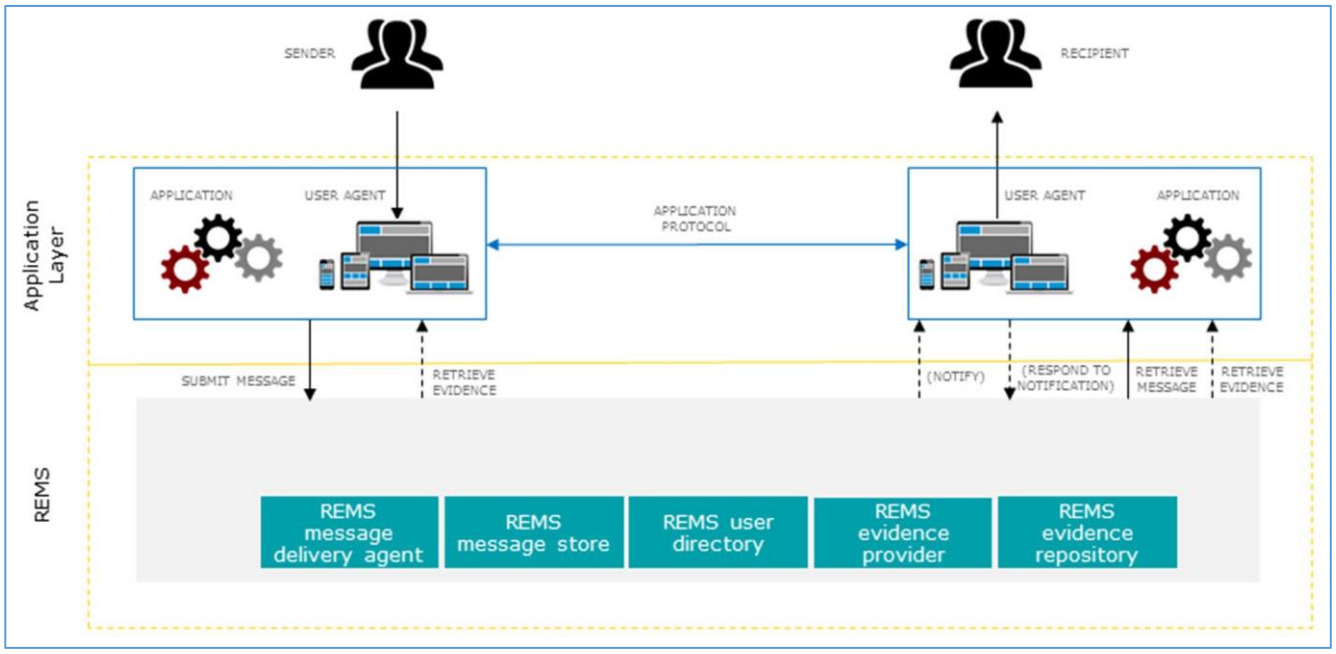
S-REMS transfers the consignment to R-REMS in a secure manner. After the consignment enters the recipient's R-REMS system, the consignment is considered handed over. At the moment of this event, the necessary evidence with integrated data about the type of event, including date, time, control/hash sum of the user content, which are electronically signed by the

QREMS signing service (QREMS SU, with object identifier: 1.3.6.1.4.1.47272.2.10.2) and signed with a qualified time stamp. The signing service uses certificate that is issued by the Certification authority in this case „Evrotrust Service CA" with OID: 1.3.6.1.4.1.47272.2.14 in the Evrotrust architecture. If no delivery to R-REMS is possible, the system also automatically generates the necessary evidence for this event.

4.3 LOGICAL MODEL OF THE PROCESS OF DELIVERY OF QUALIFIED REGISTERED ELECTRONIC MAIL SERVICE:

QREMS provides data about events that happen during the transmission of user contents (messages, documents and other objects) between the parties, e.g. evidence that the data have been sent by the sender or that they have been delivered to the recipient. This evidence can be used in order to proof to third parties or during court proceedings that the exchange of user content was conducted between the specific parties at a specific moment in time, which is confirmed by a qualified time stamp. All service users (senders and recipients) have a unique identifier that is logged in the REM messages and the evidence for ERDS. For REMS, the users' unique identifier is an e-mail address, as required by clause 5 of ETSI EN 319 532-3.

The evidence for QREMS is signed with an advanced electronic seal of the provider by the Certifying Authority for Qualified Registered Electronic Mail Service (**Evrotrust Services CA).** The evidence contains information about a specific event related to the process of data transmission between the sender and the recipient, such as successful/unsuccessful sending or successful/unsuccessful receiving of the user content, as well as the specific moment when that event occurred. The evidence for QREMS can be downloaded from the sender's/recipient's system. Evrotrust stores all evidence for a period of 10 years in a storage for later access by stakeholders.



QREMS takes place through a "user agent" - an application directly interacting with the user. The user agents/programmes (UA) via which the sender and the recipient communicate with the system for registered electronic mail service are SMTP and IMAP clients that maintain mutual TLS authentication (e.g.: Mozilla Thunderbird, etc.).

In these cases, the client software uses standard e-mail protocols (SMTP/IMAP) for access to QREMS. The sender and the recipient have a unique identifier used to identify them in REM deliveries and evidence for REMS. For QREMS, the users' unique identifier is an e-mail address, as required by clause 5 of ETSI EN 319 532-3. For the purpose of submission of user content, certain metadata are transmitted by the sender to QREMS, e.g. the e-mail address of one or more recipients, the requested work style, the delivery options, etc. These metadata are transmitted with the electronic mail consignment. The additional specification of the content and the format of the metadata is in line with ETSI EN 319 532-2 and ETSI EN 319 532-3.

The logic model illustrated on the figure presents the functionality of QREMS in individual components called "roles". The general QERDS model also applies to QREMS. The ERDS elements are described in the QERDS Policy (subsection 4.2.1 of ETSI EN 319 522-1).

REMS components that correspond to the general ERDS components:

REMS components	**Corresponding ERDS components**
REMS message delivery agent	ERDS Message delivery system
REMS evidence provider	ERDS Evidence provider
REMS evidence repository	ERDS Evidence repository
REMS user directory	ERDS User directory

In addition to the general ERDS components, REMS also provides a component for storage of REMS user content - REMS storage of user contents. The REMS storage of user content is distributed between the senders and recipients and is available for downloading.

REMS include the following main roles: REMS message delivery agent, REMS message store, and REMS evidence provider. In addition REMS include the REMS evidence repository and the REMS user directory.

4.4 OPERATIONAL PROCESS OF PROVISION OF SERVICE

Evrotrust customers access QREMS using application programs / UIs. Supported user interfaces (UIs) are:

User agents (UA)	**How QREMS is accessed**
Mozilla Thunderbird	By using an e-mail client
Mozilla Firefox	By using a web interface to access e-mail
Microsoft Internet explorer	
Microsoft Edge	
Apple Safari	
Google Chrome	

The use of the service requires initial identification of the sender and recipient, which takes place remotely through a mobile application or through the personal presence of the persons or their representatives before any of the Registration Authorities (RA) of Evrotrust. The data about

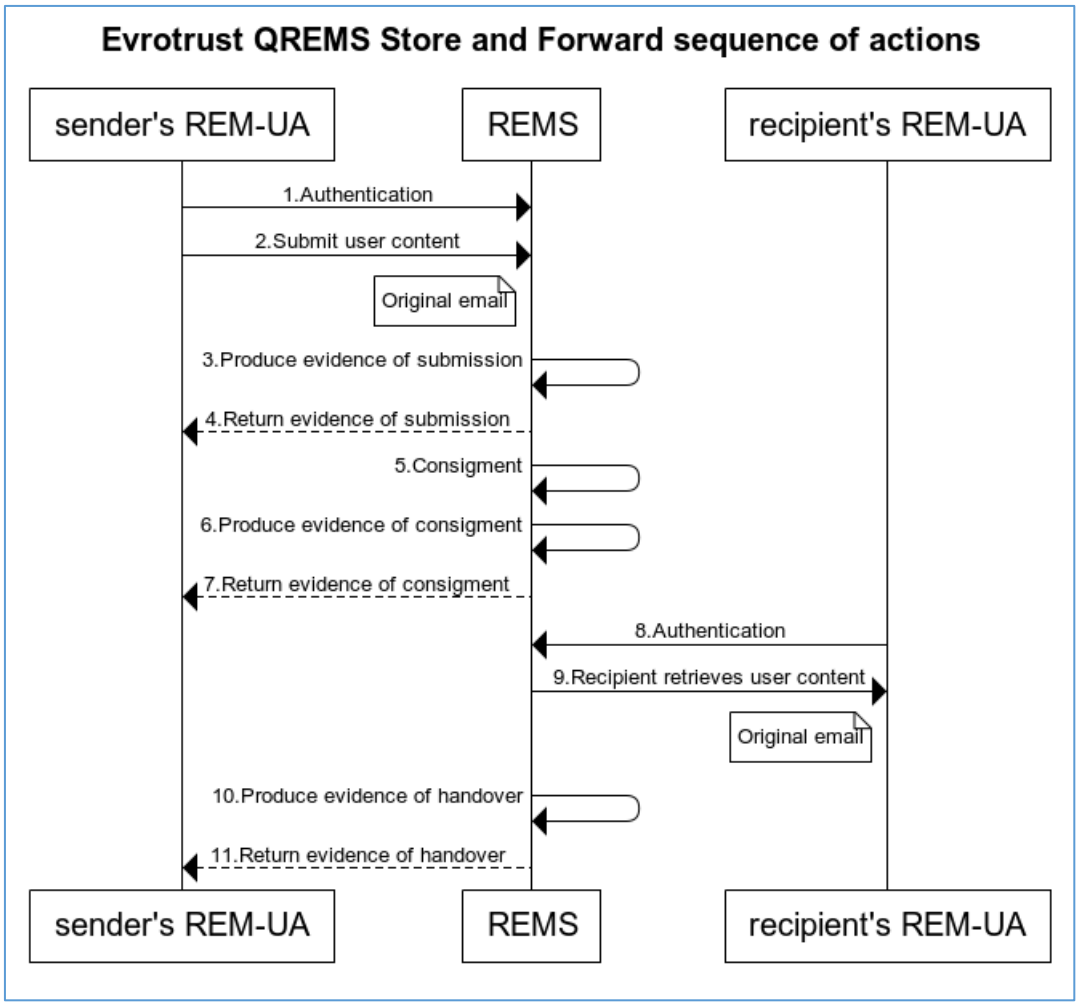
the sender and recipient collected by Evrotrust are personal data, contact details, identity document data, etc.

QREMS provides users with the opportunity to send and receive user content in MIME format. QREMS provides users with the opportunity to send user content through SMTP and to receive user content through IMAP.

The requirements of Regulation (EU) No. 910/2014 are applied for QERDSP and for QERDS for the user content, which is protected through an advanced electronic seal or signature issued by Evrotrust in a way that precludes any possibility for changes in the data without establishing this change. The date and time of sending, delivery and receiving of the user content are signed with a qualified electronic time stamp. The evidence for sending and the evidence for receipt is linked to the user content with a qualified electronic time stamp. The evidence includes a unique identifier, which is the e-mail of the individual or of the legal entity.

Evrotrust applies the Send and Forget (S&F) principle in the provision of QREMS. In this process, the user content provided by the sender is transmitted to the recipient without requesting their express consent. Evrotrust's system allows the user content to be available to the recipient for a certain period of time. After the user content is sent, no other action is required by the recipient, except for authentication.

Sequence of activities in the S&F work style, where, for the sake of simplicity, the cases of rejection are not discussed in this sequence:



1. The sender (user) is authenticated in QREMS by using an e-mail address entered in the qualified certificate for advanced electronic signature.

2. The sender (user) prepares the user content, indicates one or more recipients and provides the data to QREMS.

3. QREMS monitors the event where the user content is submitted. The system creates evidence for sending.

4. The sender optionally could receive/retrieve the evidence for sending to REMS.

5. QREMS submits the user content to the recipient's system. It also stores additional related information/metadata (e.g. sender identity, precise time of submission, etc.) and data about REMS (e.g. submission of the evidence obtained in step 3) together with the user content.

6. QREMS monitors whether the user content has been delivered to the recipient and creates evidence for consignment.

7. The sender optionally could receive/retrieve the evidence for consignment from REMS.

8. The sender (user or system) is authenticated before REMS by using an e-mail address

entered in the qualified certificate for advanced electronic signature.

9. The sender (user or system) retrieves the user content and the related metadata and/or evidence for REMS.

10. QREMS monitors whether the user content has been handed over to the recipient and creates evidence for handover.

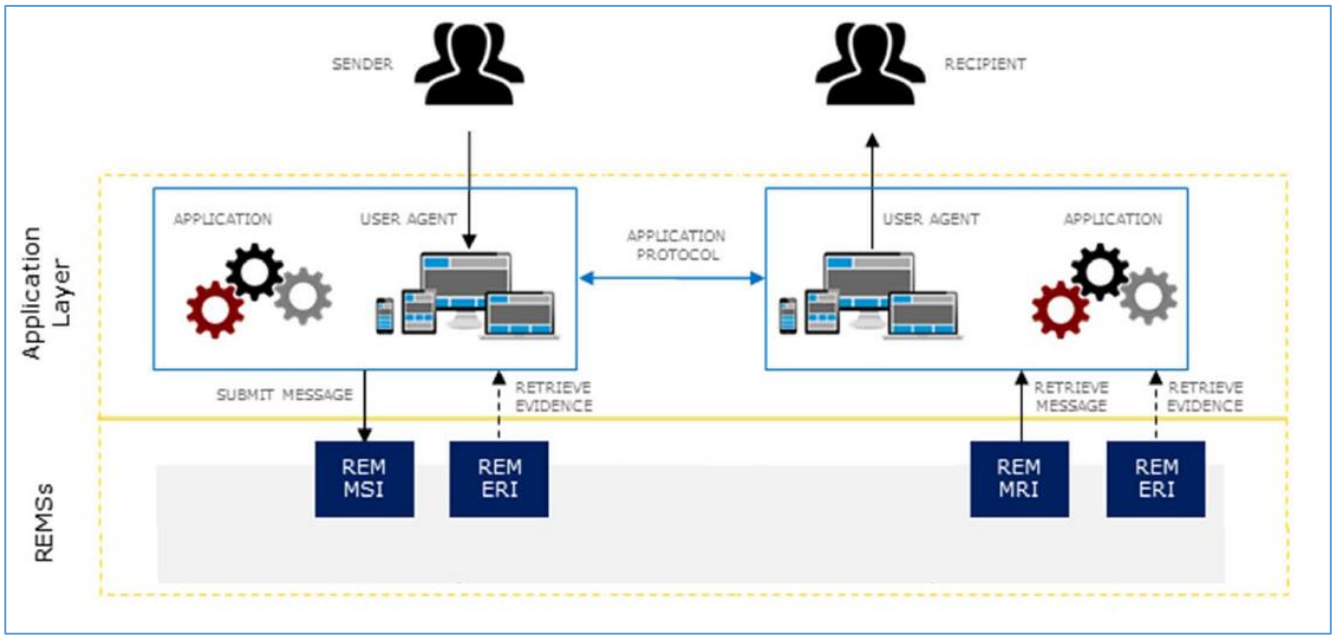
11. The evidence for handover of the content is sent back to the sender.

All evidence generated is stored by QREMS for later access upon request.

4.5 REM INTERFACES

By definition, REMS is a specific type of ERDS, which allows to apply the ERD interfaces to REM. Considering the fact that the transport mechanisms in ERDS may vary, whereas in REM they are generally based on IMAP and SMTP standards, REM interfaces have a more specific structure.

4.5.1 MODEL OF IMPLEMENTATION OF THE REMS INTERFACES



4.5.2 TYPES OF REMS INTERFACES

4.5.2.1 USER CONTENT SUBMISSION INTERFACE - REM MSI (MESSAGE SUBMISSION INTERFACE)

The REMS MSI interface is used by REM-UA/Application of the sender for forwarding the original user content to the recipient(s). REM MSI uses SMTP and TLS protocols, which provide a secure channel for the data sent. This interface requires initial identification and authentication of the sender. Evrotrust has ensured preventive measures in order to guarantee the data confidentiality and integrity.

4.5.2.2 USER CONTENT RETRIEVAL INTERFACE - REM MRI (MESSAGE RETRIEVAL INTERFACE)

This interface is used by the REM-UA/Application for retrieving user content and the relevant metadata and evidence. This interface requires initial identification and authentication of the recipient. Evrotrust has ensured preventive measures in order to guarantee the data confidentiality and integrity. Evrotrust ensures the confidentiality, integrity and authenticity of the data sent through TLS. REM MRI uses IMAP and TLS protocols.

4.5.2.3 EVIDENCE RETRIEVAL INTERFACE - REM ERI

This interface is used by the REM-UA/Application for retrieving evidence. This interface requires initial identification and authentication. Evrotrust has ensured preventive measures in order to guarantee the data confidentiality and integrity. Evrotrust ensures the confidentiality, integrity and authenticity of the data sent through TLS. REM MRI uses IMAP and TLS protocols. REM ERI uses the same channel as REM MRI.

The authentication in REM MSI relies on TLS authentication based on qualified certificates. The authentication in REM MRI and REM ERI relies on TLS authentication based on qualified certificates.

The REM MSI, REM MRI and REM ERI interfaces provide preventive measures in order to guarantee the data confidentiality and integrity. Irrespective of this, the sender may ensure the

confidentiality of the user content by encrypting the user content before sending it. In this case, the confidentiality of the user content receives additional protection outside the secure channels of these interfaces and, as a result, REMSP is unable to read the user content protected via encryption.

REMS authenticate the sender and provides evidence therefor. Irrespective of this, the sender may ensure the integrity and authorship of the user content by adding a qualified signature/seal before sending. In this case, the electronic signature will become part of the consignment and will provide the recipient with additional assurance.

4.6 SENDER/RECIPIENT IDENTIFICATION

4.6.1 SENDER IDENTIFICATION

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

4.6.2 RECIPIENT IDENTIFICATION

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

4.7 CREATION OF EVIDENCE

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

4.7.1 EVIDENCE RELATED TO THE SENDER (S-REMS)

The procedure is described in the document entitled "Qualified Electronic Registered Delivery Service Policy" AD.

REM fulfils additional requirements in the creation of evidence for REMS for each type of event. Sending is an action where the original user content coming from an external source passes

through REM MSI (message submission interface) of REMS. The procedure includes sender authentication. In REM, the initial message is the user content that shall be sent to the recipient, which is received through the system and which is REMSP responsibility. REM MSI is accessed through SMTP (Simple Mail Transfer Protocol), which is used for ensuring submission of the user content to REMS. The sender may use a user agent or a mail transfer agent. After the submission, REMS may process the submitted original user content in order to approve its acceptance; e.g. it may check it for malware, may check whether the titles of the user content are in line with the requirements for such types of messages, etc.

REMS processes the following events:

Event type under ETSI EN 319 522-1	**Relevant interface**	**Issuer of REMS**	**Implementation**
SubmissionAcceptance	REM MSI	S-REMS	REMS accepts the original user content and the REMSP undertakes the responsibility to deliver it to all designated recipients by observing the rules for delivery given by the sender.
SubmissionRejection	REM MSI	S-REMS	REMS rejects the presented user content. REMS informs the sender about the reason for rejection.

4.7.2 EVIDENCE RELATED TO THE RECIPIENT (R- REMS)

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

The submission of user content is a process where the sender's user content (the consignment) is transferred to the recipient's system which is R-REMS. The process includes successful initial identification and authentication of the recipient and use of QREMS through R-REMS. In this process, the relevant metadata and/or identification data for REMS are transferred together with the sender's content.

The delivery of the user content takes place at the recipient's system, which is R-REMS. When REM MRI is delivered through IMAP, the process includes the possibility for delivery of more than one consignment with user content. When IMAP is used for access to R-REMS, this allows retrieval only of the consignment title, without its content. REM MRI may be accessed through HTTP.

REMS issues evidence for the successful or unsuccessful transfer:

Event type under ETSI EN 319 522-1	**Relevant interface**	**REMS Issuer**	**Implementation**
ContentHandover	REM MRI	R-REMS	The user content has been successfully delivered to the recipient in their system, which is R-REMS.
ContentHandoverFailure	REM MRI	R-REMS	The user content has not been successfully delivered to the recipient in their system, which is R-REMS within a certain period of time or for other reason.

4.7.3 EVIDENCE RELATED TO THE DELIVERY

The delivery is an operation of R-REMS, which makes the user content available for the recipient and accessible to him after their authentication. The delivery is considered implemented internally by REMS, not through external interfaces. R-REMS issues evidence for successful or unsuccessful consignment for each user content to REMS. The delivery may take place by storing the user content in the recipient's system, which is an R-REMS and to which the recipient has access following authentication.

The evidence storage period is 6 months, after which it is archived for a period of 10 years. User content is stored for a period of 6 months, after which it is deleted automatically, unless it is deleted earlier by the recipient.

R-REMS issues evidence for successful or unsuccessful delivery of the user content to the recipient:

Event type under ETSI EN 319 522-1	**Relevant interface**	**Issuer**	**Implementation**
ContentConsignment	none	R-REMS	R-REMS delivers the user content to the recipient.
ContentConsignmentFailure	none	R-REMS	REMS could not deliver the user content to the recipient within a certain period of time.

In line with the terminology used in ETSI EN 319 531 and the terminology used in national legislation (EMA and EDETSA), Evrotrust's Policy specifies the consignment and handover time of user content based on the specific implementation of the QREM service:

1. by the recipient's use of **electronic mail client** (such as Mozilla Thunderbird):

   a. consignment: upon receipt in the mailbox of REM, after the recipient has indicated REM as the recipient's (addressee's) information system.

   b. handover: the time of retrieval of the consignment in the e-mail client (such as Mozilla Thunderbird) of the sender (addressee).

2. by the recipient's use of **web interface** for access to electronic mail:

   a. consignment: upon receipt in the mailbox of REM, after the recipient has indicated REM as the recipient's (addressee's) information system.

   b. handover: at the time of visualisation as a new email in the recipient's browser through the web interface.

4.8 PROTECTION OF THE DATA TRANSFERRED AGAINST ANY RISK OF LOSS, THEFT, CORRUPTION OR UNAUTHORISED CHANGES

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

4.9 TERMINATION OF A CONTRACT FOR DELIVERY OF QUALIFIED REGISTERED ELECTRONIC MAIL SERVICE

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

4.10 TRUSTED STORAGE OF PRIVATE KEY

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

5 CONTROL OF PHYSICAL AND ORGANIZATIONAL SECURITY

5.1 PHYSICAL SECURITY CONTROLS

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

5.1.1 PREMISES AND PREMISE CONSTRUCTION

Evrotrust has a specially constructed and equipped premise with the highest level of physical access control, where the Certifying Authority of Evrotrust and all central components of the infrastructure are located.

5.1.2 PHYSICAL ACCESS

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

5.1.3 ACCESS CONTROL

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

5.2 MANAGEMENT OF INCIDENTS

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

5.3 STAFF CONTROL

The organizational control implemented by Evrotrust is described in paragraph 5.2 of the document "Practice of Qualified Certification Services".

5.4 AUDIT PROCEDURE

The verification and control of the activities of Evrotrust is described in the document "Policy and practice of a qualified service for electronic mail from Evrotrust Technologies AD".

5.5 ARCHIVING

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

5.5.1 STORAGE OF DATA MEDIA

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

5.5.2 WASTE DISPOSAL

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

5.5.3 ASSET MANAGEMENT

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

4.1.1. RECORDS OF EVENTS AND KEEPING LOGS

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

5.6 CHANGE OF KEYS

The provider may change the keys of the Certification Authority "Evrotrust Services CA" and the Signatory "QREMS SU" in the case of:

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

Upon the change of the private key Evrotrust, the following rules are observed:
"QREMS SU", whose key the evidence is signed and whose key will be changed, stops issuing the certificates 60 (sixty) days prior to the moment when the remaining period of validity of the private key equals the period of validity of the last signed proof;

- The Certification Authority "Evrotrust Services CA", whose private key signs the QREMS SU certificate and the CRL and whose private key will be changed, continues to publish lists signed with the old private key to the moment when the last signed certificate expires.
- Evrotrust does not renew a user-qualified certificate requested remotely through the mobile application. Upon expiration, a new certificate is issued, with a new pair of keys.

5.7 COMPROMISE AND RECONSTRUCTION IN DISASTERS

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

5.7.1 BUSINESS CONTINUITY PLAN

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

6 CONTROLS OF TECHNICAL SECURITY

6.1 GENERALIZATION AND INSTALLATION OF KEY PAYRS

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

6.2 PROTECTION OF PRIVATE KEYS AND CRYPTOGRAPHY MODULE

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

Evrotrust has developed security controls for the management of all cryptographic keys and cryptographic devices during their entire lifecycle.

The QREMS provider generates a qualified certificate for an electronic seal which it uses for its activity related to the provision of QREMS. The electronic seal and the qualified electronic time stamp are stored in a physically isolated premise and access to the keys is granted only to authorised trusted staff. The private key for sealing by the QREMS system is stored and used in a secure environment for cryptographic operations. This key is archived, stored and recovered only by employees on trusted positions in a physically secure environment. The number of employees authorised to perform this function is minimum and corresponds to the QREMS practice. The private key for sealing by QREMS is stored in a secure protected environment of QREMSP and does not exit the environment unprotected.

QREMSP uses modern protocols and algorithms for encryption of the data transmitted.

6.3 OTHER ASPECTS OF THE MANAGEMENT OF KEY PAYRS

The procedure for the management of the key pairs of the Evrotrust services CA and the signatory of the QREMS SU is described in paragraph 6.2 of the Practice for Qualified Certification Services.

6.4 ACTIVATION DATA

The procedure for activating the key pairs of the Evrotrust services CA and the signatory of the QREMS SU is described in paragraph 6.2 of the "Practice for Qualified Certification Services".

6.5 COMPUTER SECURITY

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

6.6 SECURITY OF THE LIFE CYCLE OF THE TECHNOLOGY SYSTEM

The security procedure for the life cycle of the technology system is described in paragraph 6.6 of the document "Practice for Qualified Certification Services ".

6.6.1 INFORMATION SYSTEM VULNERABILITY ASSESSMENT

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

6.7 NETWORK SECURITY

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

6.8 TIME-STAMP

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

7 PROFILES OF QUALIFIED CERTIFICATES, CRL AND OF OCSP

The profile of the basic certification authority is described in the document "Practice of Qualified Certification Services"

7.1 PROFILE OF BASE ROOT CERTIFICATION AUTHORITY "EVROTRUST RSA ROOT CA"

The profile of the basic certification authority is described in the document "Practice of Qualified Certification Services"

7.2 PROFILE OF CERTIFICATION AUTHORITY („EVROTRUST SERVICES CA ")

The profile of the certification authority is described in the document "Practice of Qualified Certification Services"

7.3 PROFILE OF VALIDATION AUTHORITY (EVROTRUST SERVICES OCSP)

The profile of the validation authority service is described in the document "Practice of Qualified Certification Services"

7.4 PROFILE OF LIST OF CANCELLED AND TERMINATED CERTIFICATES (CRL)

Profile of the list of cancelled and terminated certificates is described in the document "Practice of Qualified Certification Services"

7.5 PROFILE OF „EVROTRUST QERDS SU“

The profile of "EVROTRUST QERDS SU" is in the document: "Practice of Qualified Certification Services"

7.6 PROFILE OF „EVROTRUST QREMS SU “

"Evrotrust QREMS SU" is a qualified certificate for the qualified electronic seal of the qualified registered electronic mail service. It electronically signs the emails, that contains evidences using a signing unit (SU) that is issued under this policy. The qualified certificate for qualified electronic seal of "Evrotrust QREMS SU" is:

Version	V3	
Serial number	5e 2c 7c b1 a8 ae ef f4 72 7d fb f5 b1 18 4a be e6 db 03 8b	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Valid from	13 July 2019, 15:38:50 UTC	
Validit to	11 July 2024, 15:38:50 UTC	
Subject	E=	qrems-ca@rem.evrotrust.com
	CN=	Evrotrust QREMS SU
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Authority Key Identifier	KeyID=1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://services.evrotrust.com/EvrotrustServicesCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name:	

<table>
<tr><td></td><td>URL=http://services.evrotrust.com/ocsp</td></tr>
<tr><td>Subject Alternative Name</td><td>RFC822 Name=qrems-ca@rem.evrotrust.com</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.10.2
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>Extended Key Usage</td><td>Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-Legal (oid=0.4.0.194121.1.2)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcSSCD (oid=0.4.0.1862.1.4)</td></tr>
<tr><td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-eseal (oid=0.4.0.1862.1.6.2)</td></tr>
<tr><td>id-etsi-qcs-QcPDS (oid=0.4.0.1862.1.5)</td><td>PdsLocations:

PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
language=en</td></tr>
</table>
</td></tr>
<tr><td>CRL Distribution Points</td><td>[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://services.evrotrust.com/EvrotrustServicesCA.crl</td></tr>
<tr><td>Subject Key Identifier</td><td>9f f0 f3 0b 8c 23 46 6e 1e 6c 9e 7a d1 4e 40 ad 11 0a 04 7c</td></tr>
<tr><td>Basic Constrains (critical)</td><td>Subject Type=End Entity
Path Length Constraint=None</td></tr>
<tr><td>Key Usage (critical)</td><td>Digital Signature, Non-Repudiation (c0)</td></tr>
</table>

Thumbprint (SHA1): b0bac1285626e8062cf6676deccb0dfb47c84ce9

Thumbprint (SHA256):

c353ebf28b34b0910d7a74e1d0211cd4220a92002d166240a6bc4c923bcf78ee

8 COMPLIANCE AUDIT AND OTHER ASSESMENT

The procedure for carrying out the compliance audit is described in paragraph 8 of the document "Practice of Qualified Certification Services".

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 TARIF

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

9.2 FINANCIAL RESPONSIBILITY

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

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

9.3 PERSONAL DATA PRIVACY

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

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

1) The company uses in its activities:

- only such information about the activities and the business of its customers and partners that is required to provide QERDS;
- confidential information such as commercial, financial and technical documents (software, analyzes, tables, data, surveys, prices, contracts and other documents).

2) Evrotrust informs its employees:

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

- of the provisions of the Personal Data Protection Act and the European legislation on personal data protection, as well as the measures and procedures for the protection of personal data in the company;
- that all data and information defined as constituting trade secret shall be carefully stored to prevent disclosure without the express permission of the provider;
- that they are obliged to collect personal data regardless of the ethnicity of the person to whom they relate and regardless of their form and location. They are obliged to protect the data from deliberate or accidental destruction, deletion, transmission to third parties or other type of processing of such data;
- that processing of personal data (collection, storage, modification, transmission, deletion and any type of processing related thereto) is only permitted in cases where there is legal grounds for such processing in accordance with national legislation governing the protection of personal data and that any other type of processing is illegal;
- that unauthorized disclosure of confidential information lies at the root of the cessation of cooperation;
- that the issuance and unwarranted acquisition of professional secrecy constitutes a crime;
- that misuse of personal data constitutes a crime.

9.4 INTELLECTUAL PROPERTY RIGHTS

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

9.5 OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES

9.5.1 OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES OF EVROTRUST

Evrotrust warrants that it performs its activities by:

- complying with the terms and conditions of this document, the requirements of Regulation (EU) No. 910/2014 and the national legislation;
- its provided QERDS service not infringing the copyrights and licensed rights of any third party;

- using technical equipment and technologies that ensure system reliability and technical and cryptographic security in the performance of the processes, including a secure and protected mechanism/device for generating keys in its infrastructure;
- providing QERDS after verifying the information provided by means permitted by law;
- securely storing and maintaining information related to the QERDS provided and the systems operational performance;
- complying with the established operational procedures and the technical and physical control regulations, in accordance with the terms and conditions of this Policy and the "Certification practice statement for qualified certification services";
- providing conditions for the accurate determination of the time of sending and receiving data;
- performing procedures of identification and authentication of natural and legal persons or of authorized representatives of legal persons;
- taking immediate measures in the event of technical security issues;
- informing customers about their obligations and due care in the use of the QERDS certification service provided by Evrotrust;
- using and storing the collected personal and other information only for the purposes of its activities in accordance with the national legislation;
- maintaining disposable funds, which enable it to carry out its activities;
- concluding an insurance for the period of its activities;
- maintaining trusted staff having the necessary expertise, experience and qualifications to perform the activities;
- maintaining a Public Register in which it publishes electronic documents related to its activities;
- providing permanent access to the Public Register by electronic means (24/7/365);
- ensuring protection against the introduction of changes to the maintained Public Register from unregulated or unauthorized access or due to a random event;
- performing periodic internal audits of the activities of the Certification Authority and the Registration Authority;
- performing external audits by independent auditors and publishing the audit results on its website;
- using in its activities certified software and hardware as well as secure and reliable

technology systems;

- maintaining on the Evrotrust website a list of registration authorities, a list of recommended software and hardware for customer use, templates, forms, sample Agreement and other documents for the benefit of customers;
- providing maximum access to its services (365/24/7), except for the following cases:
  - scheduled and pre-announced technical repairs to the infrastructure;
  - unscheduled technical repairs to the infrastructure as a result of unforeseen failures;
  - maintenance due to infrastructure failures beyond the provider's jurisdiction;
  - inaccessibility of the service as a result of force majeure or extraordinary events.
- declaring the maintenance or upgrading of its infrastructure at least three (3) days prior to the commencement of the repair.

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

- resulting from failure to comply with the requirements of Regulation (EU) No. 910/2014 in the performance of its QERDS provision activities;
- resulting from failure to comply with its obligations to provide QERDS;
- resulting from faults in establishing the original identity of customers.

9.5.2 OBLIGATIONS, RESPONSIBILITIES AND WARRANTIES OF THE REGISTRATION AUTHORITY

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

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

Evrotrust warrants that the Registration Authority:

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

9.5.3 OBLIGATIONS OF SENDERS AND RECIPIENTS

Natural and legal persons shall have the following obligations:

- to become acquainted with and comply with the terms and conditions of the Agreement, the General Terms and Conditions, Policies and Practices when using QERDS, as well as the requirements in the other documents published in the Public Register of Evrotrust;
- to use the qualified electronic registered delivery for legitimate purposes only and in accordance with its Policy and Practice;
- to agree with the terms and conditions set out in the Agreement between them and Evrotrust.

9.6 RELEASE FROM LIABILITY

Evrotrust IS NOT liable for damages arising from:

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

9.7 LIMITATION OF LIABILITY

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

9.8 ACTIVITY INSURANCE

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

9.9 TIME AND TERMINATION OF POLICY AND PRACTICE

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

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

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

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

9.10 INDIVIDUAL MESSAGES AND MESSAGES WITH PARTICIPANTS

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

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

9.11 POLICY AND PRACTICE AMENDMENTS

Changes in this document may result from observed errors, updates and suggestions from

affected parties. In the event of an invalid Policy and Practice clause, the validity of the entire document is retained and the contract with the cusmer is not violated. The invalid clause is replaced by a legal norm.

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

9.12 DISPUTE SETTLEMENT

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

9.13 APPLICABLE LAW

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

9.14 COMPLIANCE WITH APPLICABLE LAW

Evrotrust warrants that the service operates legally and reliably. It is offered in accordance with the applicable legal requirements. Any issues not settled by this document shall be governed by the provisions of the Bulgarian legislation. In the event that national legislation changes, the legal rules shall apply until the harmonization of this Policy.

Evrotrust warrants that personal data are processed in accordance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation/GDPR).

Wherever possible, the electronic registered delivery service and the end-user products used in the provision of the service are accessible to disabled people.

9.15 GENERAL PROVISIONS

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

9.16 OTHER PROVISIONS

The practice does not specify any other provisions.

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