ISO 9001:2015 ISO 27001:2022
ISO 20000-1:2018 ISO 22301:2019
Regulation (EU) 910/2014
Regulation (EU) 2016/679

QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE POLICY AND PRACTICE

TABLE OF CONTENTS

1 INTRODUCTION

Evrotrust Technologies AD (Evrotrust) is a qualified trust service provider operating 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 on the internal market and repealing Directive 1999/93/EC (Regulation (EU) No. 910/2014) and the Electronic Document and Electronic Certification Services Act and as such entered in the European Certification Service Providers Trusted List (https://webgate.ec.europa.eu/tl-browser/#/tl/BG), as well as in the register of Bulgarian Certification Service Providers managed by the Communications Regulation Commission (http://crc.bg/files/_bg/Register_site_bg_30092017_Last_LAST.pdf).

Evrotrust provides its users with a highly reliable and secure qualified electronic registered delivery service in accordance with Regulation (EU) No. 910/2014.

1.1 OVERVIEW

The "Qualified Electronic Registered Delivery Service Policy and Practice" (Policy and Practice) is a document that describes the general rules and norms applied by Evrotrust Technologies AD (Evrotrust) for the provision of a Qualified Electronic Registered Delivery Service (QERDS). The document relates to a certification service of Evrotrust, under Section 7 of Regulation (EU) No. 910/2014, and in accordance with the applicable legislation in the Republic of Bulgaria.

This document defines the generally applicable requirements for the activities of Evrotrust in its role as Qualified Electronic Registered Delivery Service Provider (QERDSP). The policy regulates the provisions concerning the company staff (competencies, responsibilities, empowerment and duties depending on the role of each employee).

The Qualified Electronic Registered Delivery Service (QERDS) is a specific type of ERDS (Electronic Registered Delivery Service). In QERDS, both the service and its provider shall meet a number of additional requirements which do not need to be met by regular ERDS providers. QERDS allows for the sending and/or receipt of user content (electronic documents) and secure and long-term storage of the evidence for this process. This service is a convenient tool for quick and reliable delivery of information. Evrotrust provides security and protectability of communication along with certification of the time of sending documents and messages from the

sender and certification of the time of receipt of documents and messages from the recipient, as well as evidence of the communication that ensure the authenticity of the documents exchanged. Evrotrust provides secure initial identification of the recipient and the sender and protection against loss, theft, damage or unauthorized modification of the transmitted data whereby it ensures the integrity of the messages.

The service is intended for natural and legal persons, administrations, persons performing public functions, and public service organizations.

Becoming acquainted with the objectives and role of the Policy and Practice is particularly important for Evrotrust users in view of the applicability of this service.

The relationship between Evrotrust and the end-user are governed by the General Terms and Conditions of the Contract for Trust, Information, Cryptographic and Other Services.

This document is complied with the standard ETSI EN 319 521 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers.

The document is a public document. It can be amended by Evrotrust at any time, and any new revision shall be approved by the Board of Directors and communicated to interested parties through the company's website.

This document is an integral part of the policies and practices for the provision of qualified services of Evrotrust.

1.1.1 LEGAL REFERENCES

The Policy and Practice is complied with the following documents:

- 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;
- ETSI TS 119 461 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".

1.2 NAME AND IDENTIFIER OF THE DOCUMENT

This document has the full title "Qualified electronic registered delivery service policy and practice" of Evrotrust Technologies AD and an identifier:

Policy Name	Object ID Number (OID)
QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE POLICY AND PRACTICE	1.3.6.1.4.1.47272.2.10.1

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. If there is an extension/update in policy and practice that will not affect previously issued certificates, Evrotrust presents a new object identifier that covers the new certificates or extended/updated ones. Evrotrust follows an internal OID management procedure.

1.3 PARTICIPANTS IN INFRASTRUCTURE

1.3.1 CERTIFYING AUTHORITIES

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

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

1.3.1.2 OPERATIONAL CERTIFIED AUTHORITY (EVROTRUST SERVICES CA)

"Evrotrust Services CA" is the certifying authority of the qualified electronic mail service which, by using the signing unit "Evrotrust QERDS SU", electronically signs the evidence issued under this policy.

1.3.1.3 CERTIFICATE STATUS AUTHORITY "EVROTRUST SERVICES VALIDATION"

"Evrotrust Services Validation" is the validating authority of the qualified electronic mail service which signs the status certificates issued by Evrotrust Services CA. The status verification service is accessed via OCSP protocol.

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

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

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

1.3.2 REGISTRATION AUTHORITY

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

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

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

1.3.3 USERS

Any natural or legal person who has a contract with Evrotrust for a qualified electronic registered delivery service is a QERDS user.

Users can use the qualified registered delivery service (electronic delivery/handover) as senders and/or recipients.

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

1.3.4 TRUSTING PARTIES

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

In this case, they are not QERDS users.

1.3.5 OTHER PARTICIPANTS

Evrotrust reserves the right to enter into contracts with external parties for the provision of certain certification services, where necessary.

1.4 APPLICABILITY OF ELECTRONIC REGISTERED DELIVERY

QERDS is used to send and receive user content. Due to the wide range of application of the service, it is prohibited to provide it in violation of applicable regulations, standards and recommendations or beyond the scope of authorized use specified in this document. Electronic registered delivery should not be used in a manner inconsistent with its stated purpose, its scope / policy and for unlawful purposes.

The products and services provided by Evrotrust for end users are also accessible to people with disabilities.

1.5 MANAGEMENT OF POLICY AND PRACTICE

1.5.1 MANAGEMENT POLICY ORGANIZATION

Evrotrust is responsible for managing this Policy and practice.

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 is published after approval by the Evrotrust Board of Directors.

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

Contact person for managing the document "Policy and practice in the provision of Qualified Electronic Registered Delivery Service by Evrotrust Technologies AD" is the Executive Director of Evrotrust.

Further information can be obtained at the following address:

Evrotrust Technologies AD

Sofia, 1766

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

Contact telephone number: + 359 2 971 44 61 – information/Registration Authority/Technical Support

Website: http://www.evrotrust.com

E-mail: info@evrotrust.com

1.6 DEFINITIONS AND ABBREVIATIONS

1.6.1 DEFINITIONS

Electronic Registered Delivery Service/ERDS - a service that allows for the transmission of data between persons by electronic means, provides evidence regarding the processing of the transmitted data, including evidence of the sending and receipt of the data, and protects the transmitted data against the risk of loss, theft, damage or unauthorized modification;

Qualified Electronic Registered Delivery Service/QERDS – an electronic registered delivery service that complies with the requirements provided for in Article 44 of Regulation (EU)

No. 910/2014;

Electronic Registered Delivery Service Provider - a provider of qualified trust service that provides an electronic registered delivery service;

Qualified Electronic Registered Delivery Service Provider/QERDSP – a qualified trust service provider providing qualified electronic registered delivery service in accordance with Regulation (EU) No. 910/2014;

ERDS evidence - data generated within an electronic registered delivery service that are intended to evidence that a particular event has occurred at a particular time;

User Content - original data created by the sender to be delivered to the recipient;

UA/User Agent – programs (applications) through which the sender and the recipient communicate with the electronic registered delivery system;

Recipient - a natural or legal person to whom user content is addressed;

Sender - a natural or legal person providing user content;

Consignment Delivery – where the delivery of user content has crossed the boundary of the electronic registered delivery, that is, it is already available to the recipient;

Handover – where the user content has successfully crossed the boundary of the recipient's electronic registered delivery, that is, to the recipient's agent/the user's ERD application;

Original message – user content and metadata to be sent;

Consignment – sent/received content (document(s)).

1.6.2 ABBREVIATIONS

EDECSA – Electronic Document and Electronic Certification Services Act;

QTSP – Qualified Trust Service Provider;

ERD – Electronic Registered Delivery;

ERDS - Electronic Registered Delivery Service;

QERDS – Qualified Electronic Registered Delivery Service;

ERDSP - Electronic Registered Delivery Service Provider;

QERDSP – Qualified Electronic Registered Delivery Service Provider;

UA – User agent used by the sender/recipient to send/receive user content;

R-ERDS - The recipient's Qualified Electronic Registered Delivery Service System;

S-ERDS – The sender's Qualified Electronic Registered Delivery Service System.

2 RESPONSIBILITY FOR PUBLICATION AND STORAGE

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

Evrotrust publishes on its website notifications related to its activities and all important documents of interest to users and trusting parties.

Customers and relying parties are informed about the Policy and practice and the General Terms and Conditions for providing the service for electronic mail prior to signing a contract. The documentation, including Policy and practice, agreements, models, audit reports, etc. is published on the Evrotrust website immediately on each update. The operational certificates of the certifying authority are published immediately upon each issue of new certificates.

Evrotrust offers services related to access to the information stored in the storage (the public register) by providing HTTP/HTTPS based access to it.

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

3 IDENTIFICATION AND CERTIFICATION OF IDENTITY

3.1 NAMES

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

3.2 INITIAL VERIFICATION OF IDENTITY

The Evrotrust system for QERDS allows sending user messages and attached documents/files (user content) as consignments. The difference with the simple electronic delivery is that the sender and the recipient must first undergo an initial identification process before using the system. In the process of service, the sender of electronic documents is authenticated and only after that he sends the consignment, and respectively the recipient has access to its content after it has been authenticated too.

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

a) remotely using means of electronic identification which is equivalent to the physical presence of the natural or legal person. The means of electronic identification meet the

requirements referred to in Article 8 of Regulation (EU) No. 910/2014 with respect to the "significant" or "high" security levels.

For the purpose of customer identification, Evrotrust uses a remote video identification system via a mobile device that allows the provider to initially identify and remotely verify the identity of a person. In this system, the provider communicates with the national primary registers (civil registration, personal documents, corporation registers, etc.). After verification of the data provided, data are generated about the identity of the persons and they are stored in the Evrotrust for a period of 10 years. After verification of the information provided, identity / identity data shall be generated for the persons who have been retained in the Evrotrsut repository for a period of 10 years, including after termination of their activities. Evrotrust fulfills the requirements under Art. 24 of Regulation (EU) No 910/2014 by retaining all relevant information in order to provide evidence in court proceedings and to ensure continuity in the provision of the service, the period of 10 years has been determined in accordance with Art. 21 (3) of the Electronic Document and Electronic Certification Services Act.

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

3.2.1 ESTABLISHING THE IDENTITY OF A NATURAL PERSON

The establishment and initial verification of the identity of a natural person is performed automatically by remote verification and/or by a Registration Authority.

The minimum set of data for a natural person shall contain the specific data listed below:

a) family name (or names);

b) personal name (or names);

c) date of birth;

d) national unique identifier, if any, in accordance with the technical specifications for cross-border identification purposes, to remain unchanged for as long as possible. For the Republic of Bulgaria this is the personal identification number (PIN).

The minimum set of data for a natural person may also contain additional specific data:

a) personal name (or names) and family name (or names) at birth;

b) place of birth;

c) permanent address;

d) other details.

For the purposes of automated establishment and initial verification of the identity of a natural person by remote verification, the following is required:

- the natural person is required to have the mobile application of Evrotrust installed and to have initiated a registration and remote electronic identification process via a mobile device for the purpose of concluding a certification services contract with Evrotrust;
- the person must have a valid ID document scanned with the camera of a mobile/smart device (smartphone, tablet);
- Evrotrust initiates a procedure for verification of the validity of the ID document through a national ID document database (subject to appropriate integration) or uses a service for their verification;
- a procedure of automated biometric face analysis is performed by a series of controls aimed at establishing the identity of the person with the captured photograph obtained from a reliable source, including a 3D object check (using a certified methodology);
- upon failed automated verification, the next step is identification via video conferencing with an Evrotrust operator using a certified methodology for verifying the knowledge of certain personal data and visual identification of the person against the documents taken and the data received from primary registers;
- upon successful verification of the person, it signs services usage agreement available through the application of Evrotrust Technologies AD. Upon failed verification, the person is advised to visit an office of Evrotrust or its Registration Authorities for personal appearance and personal identification.

Evrotrust performs verification of the authenticity of the information using all legally permitted means in the relevant public registers.

3.2.2 ESTABLISHING THE IDENTITY OF A LEGAL PERSON

The establishment of an initial identity of a legal person is performed by a representative of the Registration Authority through automated verification in primary registers (for example: Commercial Register), check in the relevant registers by the national identifier and/or other data

given.

The minimum set of data for a legal person shall contain the specific data listed below:

a) name of the legal person (company);

b) unique national identifier in accordance with the technical specifications for cross-border identification purposes, to remain unchanged for as long as possible. For the Republic of Bulgaria this is UIC/BULSTAT.

The minimum set of data for a legal person may also contain additional data:

a) business address;

b) VAT registration number;

c) tax number;

d) identification code under Article 3 (1) of Directive 2009/101/EC of the European Parliament and of the Council (1);

e) the legal entity identifier (LEI) referred to in the Commission Implementing Regulation (EU) No. 1247/2012 (2);

f) the economic operator registration identification number (EORI number) referred to in the Commission Implementing Regulation (EU) No. 1352/2013 (3);

g) the excise number provided for in Article 2 (12) of the Council Regulation (EU) No. 389/2012 (4);

h) other details.

Evrotrust takes steps to minimize the risk that the identity of a legal person will not match the stated one.

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

The establishment of the initial identity of a natural person authorized by a legal person is performed automatedly by remote verification and/or by the Registration Authority.

In order to establish the initial identity of a natural person who is a representative of a legal person (managers, board members, procurators, etc.), where its representative power derives from a law, a check is performed in the relevant registers where such integration exists (Commercial Register, Register of Non-Profit Legal Entities, etc.).

Empowerment must come from a person with statutory representative power. Where the

representative power derives from a statement of empowerment, the same shall be submitted to and verified by Evrotrust.

For each of the natural persons, an initial identity verification is performed following the procedure described in the preceding sections.

Where the representative power cannot be established under the procedure described in the preceding rules, the original identity of the legal person will be verified on the basis of documents submitted by the Registration Authority at an office of Evrotrust.

In such a case, the following documents are required:

- notarized power of attorney or registration document, which gives rise to legal representative power (certificate of good standing, etc.);
- review and confirmation of the identity document of a natural person by performing a check in a national register;
- check of the entries of the representative power of the legal person in official registers (at the Registry Agency)
- other documents.

The initial verification of the identity of a legal person aims to evidence that during the review of the application the legal person exists and that the representative who applies for the use of QERDS has representative power.

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 QERDS 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 using a Mobile application, the person uses for authentication cryptographic keys (secrets) that are integrated into the mobile application;

2. If a person uses an API, it is provided with a secure channel cryptographic key (secret) through which it is authenticated to the system. In addition, the person only generates a pair of cryptographic keys, where the public key being used to encrypt the data to the person;

3. If the person uses a web portal, it is authenticated by the Mobile application under p.1. It is permissible for the person to be provided for the purposes of authentication and a pair of

cryptographic keys with a certificate attached to them for a qualified electronic signature which are generated and issued by a standard procedure for Evrotrust.

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

4 SERVICE PROVISION PROCESS

QERDS allows for the transfer of user content (for example: documents) between a particular sender and recipient - Evrotrust users. This service provides evidence of the integrity and timing of the transmitted data, including evidence of the sending and the receipt thereof. The service protects the data against loss, theft, damage of their integrity or unauthorized modification and meets the requirements of QERDS under Regulation (EU) No. 910/2014.

When using QERDS, the principle that the legal force of an electronic document may not be contested on the grounds that it is in electronic form is complied with, in order to ensure that an electronic transaction will not be rejected solely on the grounds that a document is in electronic form. In this regard, it is assumed that the electronic documents transmitted and received through QERDS are exhaustive, sent by the sender and received by the recipient and that the date and time of sending and receiving are accurate.

4.1 REQUIREMENTS TO THE QUALIFIED ELECTRONIC REGISTERED DELIVERY SERVICE

The QERDS service provided by Evrotrust meets all the requirements of ETSI EN 319 401, paragraph 6.1 as well as the following specific requirements:

- ERDS policies and practices are approved by the ERDSP management and communicated to stakeholders by making them available on the Evrotrust website (p.1.1);
- The ERDSP has a procedure for reviewing and updating the practices and a procedure for notifying the changes made to the interested parties (item 9.11);
- The QERDS service is provided by "Evrotrust Technologies AD". There are no other external organizations outside this organization to support the provision of the service;
- The communication on which the data is flowing is reliably protected by an encrypted channel, eliminating the risk of any changes to user content before sending / transmitting. Evidence related to the sending / forwarding of user content events is reliably stored by subsequent loss and theft in a protected environment under the control of Evrotrust for 10

(ten) years (point 4.8).

- This document (item 4.6) describes the process of identifying the sender and recipient;
- Evrotrust guarantees the identification/authentication of the sender prior to sending the user content;
- Evrotrust guarantees the identification/authentication of the recipient prior to data delivery (consignment/user content);
- the sending and the receipt of data is secured through an Evrotrust advanced electronic seal in a way that excludes any possibility of unnoticed data modification;
- this document includes the obligations (point 9.6) of the sender, recipient and relying parties;
- This document specifies the types of supply-related events and provides evidence of the process (clauses 4.5 and 4.7.3);
- any data modification required for the purpose of sending or receiving the data is clearly indicated to the sender and the recipient of the data;
- the date and time of sending, receiving and changing the user content is indicated by a qualified electronic time stamp;
- the availability, integrity and confidentiality of the user content is guaranteed from its sending to its acceptance;
- the integrity of the user content is protected, especially when exchanged between the sender/recipient or between the distributed system components of the service;
- the evidence relating to the activities of user content delivery is protected by an advanced electronic seal issued by Evrotrust, which excludes the possibility of data being modified;
- the sender specifies in advance the period of time within which the QERDS system will attempt to deliver the user content. If the sender does not select an option, then this period will be 3 days by default;
- in cases where modifications are required to the user content by ERDS these modifications are clearly indicated to the sender, the recipient and any third parties;
- The date and time of sending, receiving and changing user content are indicated by a qualified electronic time stamp;

- QERDS uses qualified services of QCSP Evrotrust Technologies AD for the issuance and management of Qualified Certificates (X.509) and Qualified Time Stamps;
- all QERDS delivery information is stored for a period of 10 years, in compliance with the national legislation of the Republic of Bulgaria (EDECSA);
- This document describes the events where delivery to R-ERDS is not possible. In such cases, the system automatically generates the necessary evidence for this event and is stored for ten (ten) years (p.4.2);
- This document clearly and unambiguously indicates that ERDS policy is in line with Regulation (EU) No 910/2014;
- This document includes the full list (p.1.3) of QTSP participants providing QERDS;
- This document includes all limitations (p.9.6) for the use of QERDS;
- Eurotrust keeps the evidence reliably from subsequent loss and theft in a protected environment for a period of 10 years;
- The possibility of terminating the service is available 24 hours a day (p.4.9).

4.2 TECHNOLOGY DESCRIPTION

QERDS uses technology that, after initial identification of the sender and its current authentication, the user content is accepted by S-ERDS on a reliably protected and encrypted secure channel. At this point, S-ERDS generates the necessary evidence, including accurate data on the type of event, including date, time, control/hash sum of the user content, electronically signed by the Certification Authority for QERDS and stamped with a qualified time stamp. If acceptance by S-ERDS is not possible, it will again automatically generate the necessary evidence of the rejection.

S-ERDS reliably transfers the consignment to R-ERDS. The necessary evidence is again generated automatically, including accurate data on the type of event, including date, time, control/hash sum of the user content, electronically signed by the Certification Authority for QERDS and stamped with a qualified time stamp. If delivery to R-ERDS is not possible, the system will automatically generate the necessary evidence of this event.

At the time when the user content reaches the recipient's system, that is, it has been handed over to the recipient, the R-ERDS generates the necessary evidence, including accurate data on the event, including date, time, control/hash sum of the user content, electronically

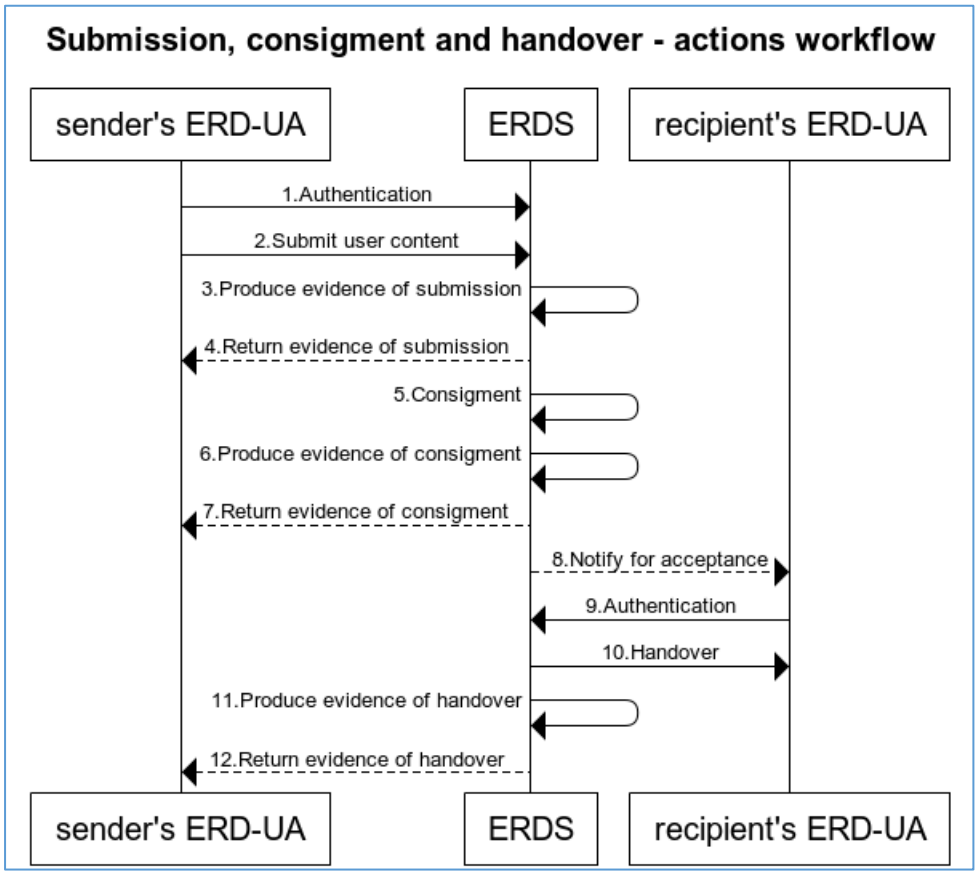
signed by the QERDS SUs and stamped with a qualified time stamp. The signing service QERDS SUs uses certificate that is issued by the Certification authority in this case „Evrotrust Service CA" with OID: 1.3.6.1.4.1.47272.2.14 in the Evrotrust architecture. If handover is not possible, R-ERDS will automatically generate the necessary evidence of this event.

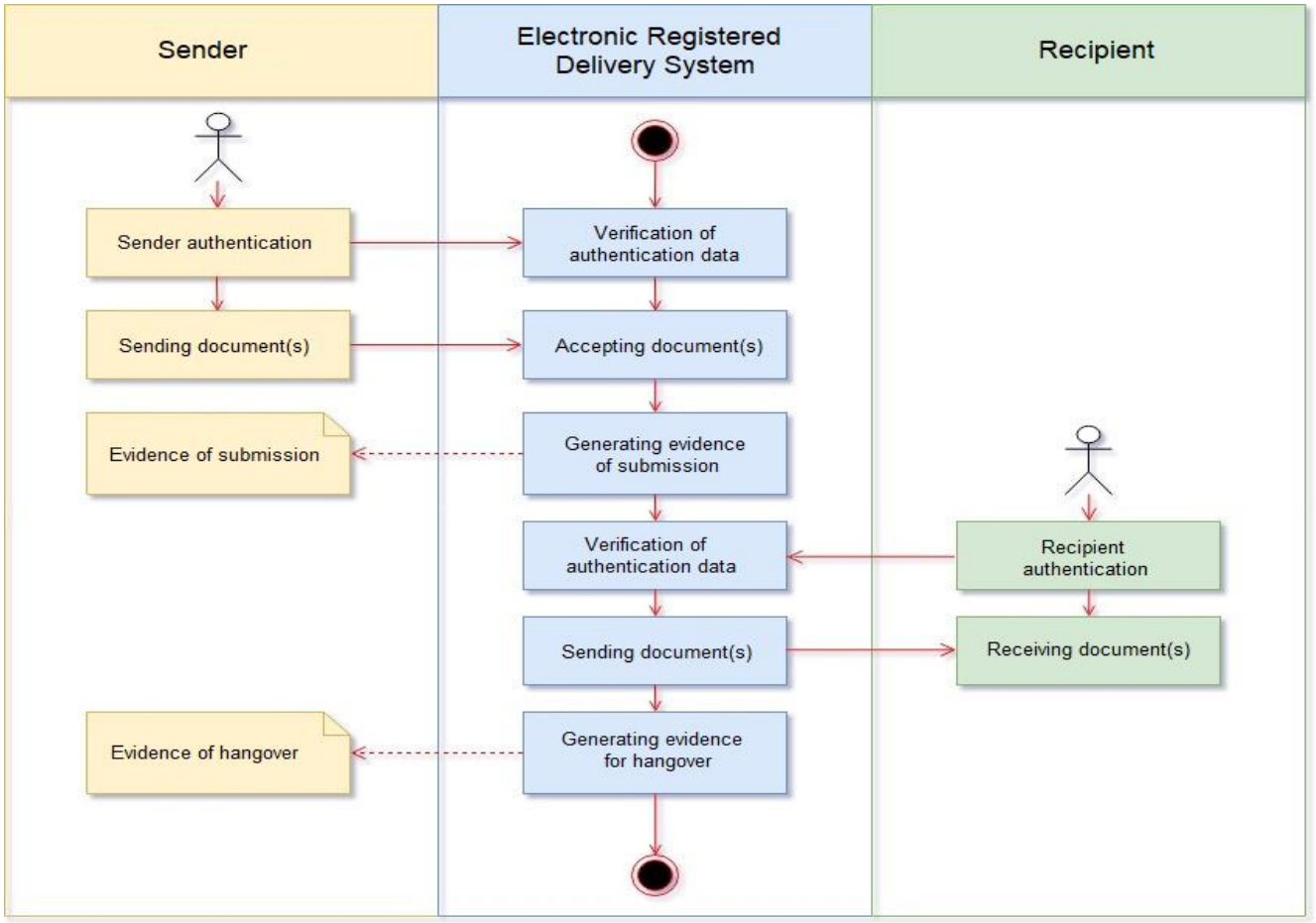
4.3 SCHEMES OF THE PROCESS OF PROVIDING A QUALIFIED SERVICE FOR ELECTRONIC REGISTERED DELIVERY

QERDS provides evidence of events that occur during the transmission of user content (messages, documents, files, and other items) between the parties (for example, information that the data have been sent by the sender or delivered to the recipient). Such evidence may be used to prove to third parties, and also in court proceedings, where necessary, that the exchange of messages or documents was made at a specific moment of time, which is confirmed by a qualified time stamp.

The evidence of QERDS is a certificate signed with an Evrotrust advanced electronic seal by QERDS Sus with object ID number: 1.3.6.1.4.1.47272.2.10.1. The certification authority of a qualified electronic registered delivery service "Evrotrust Services CA" signs the certificate of signing authority QERDS Sus. The evidence contains information that a particular event related to the data transmission process between the sender and the recipient (for example, sending or receiving a message) occurred at a specific moment of time. An item of evidence of QERDS may be immediately delivered to the sender/recipient, but it is also stored for a period of 10 years in the storage of Evrotrust for subsequent access by interested parties in compliance with the national legislation of the Republic of Bulgaria (EDECSA).

For the purpose of secure and reliable delivery of data between the recipient and the sender, Evrotrust uses initial identification of process participants. Initial identification is performed through verification of a set of identifying attributes that uniquely identify individuals.


Submission, consigment and handover - actions workflow
sender's ERD-UA
ERDS
recipient's ERD-UA
1.Authentication
2.Submit user content
3.Produce evidence of submission
4.Return evidence of submission
5.Consigment
6.Produce evidence of consigment
7.Return evidence of consigment
8.Notify for acceptance
9.Authentication
10.Handover
11.Produce evidence of handover
12.Return evidence of handover
sender's ERD-UA
ERDS
recipient's ERD-UA

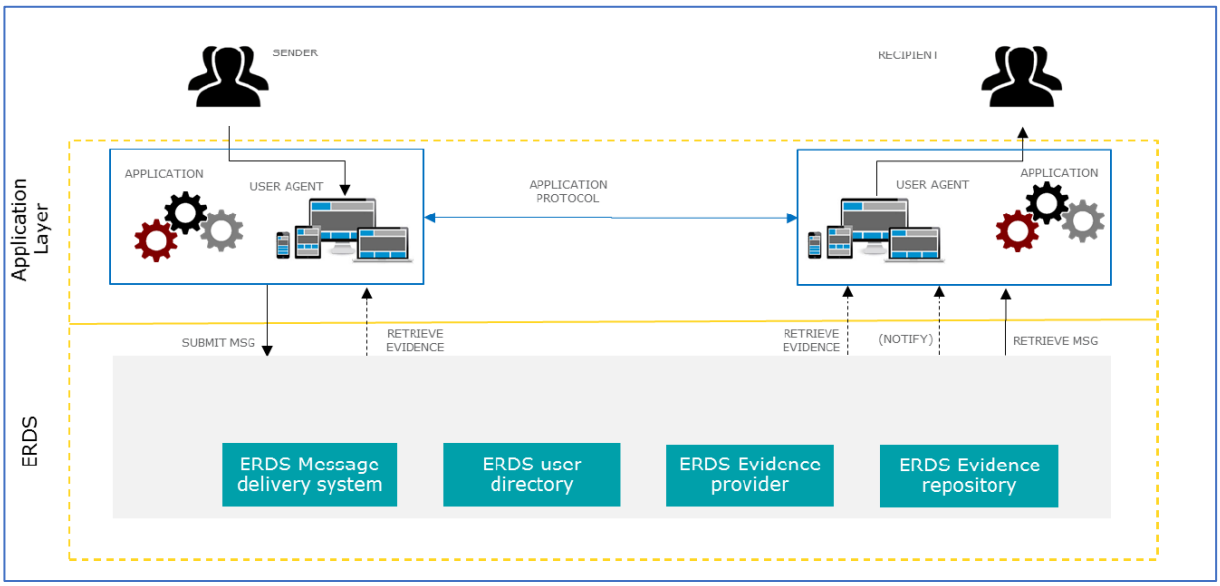

Sender
Electronic Registered Delivery System
Recipient
Sender authentication
Verification of authentication data
Sending document(s)
Accepting document(s)
Evidence of submission
Generating evidence of submission
Verification of authentication data
Recipient authentication
Sending document(s)
Receiving document(s)
Evidence of hangover
Generating evidence for hangover

4.4 PROCESS OF PROVISION OF THE SERVICE

QERDS of Evrotrust is accessed through the use of a web portal, an Application Programming Interface (API) or a mobile application. The use of the service requires the initial identification of the sender and the recipient to be performed remotely by using a mobile application or by personal appearance of the persons or their representatives before some of the Evrotrust Registration Authorities (ROs). The sender and recipient data that Evrotrust collects are personal data, contact details, identity card details and others.

The user agents/programs (UA) through which the sender and the recipient communicate with the electronic registered delivery system are:

1. Mobile application installed on a personal mobile device (mobile phone, tablet, etc.);
2. Application Programming Interface (API) through which integrated external systems use the service (companies, banks, corporations, etc.);
3. Web portal through which users use the service.



Considering the terminology used in ETSI EN 319 521 and the terminology used in the national legislation (E-Government Act and EDECSA), the Evrotrust Policy specifies the consignment delivery time and the time of handover of user content depending on the service delivery. The consignment delivery time is the time when ERDS makes the consignment

accessible to the recipient within the ERDS. The time of handover is:

- when using a mobile application: the time of delivery/retrieval of the consignment at the backend of the recipient's mobile application, which backend is a part of the recipient's user agent/application;
- when using API integration: the time of delivery/retrieval of the consignment at/from the recipient's information system using API integration;
- when using a web-based portal: the time of delivery/retrieval of the consignment at the backend accessible via the web-based portal, which backend is a part of the recipient's user agent/application.

4.5 IDENTIFICATION OF SENDER/RECIPIENT

4.5.1 IDENTIFICATION OF SENDER

Evrotrust performs initial identification of the **sender** in one of the following ways, depending on the user agent it uses:

1. When using a mobile application - the provider's registration authority first identifies the sender through the video identification system certified as secure electronic identification within the meaning of Regulation (EU) No. 910/2014. By using two-factor identification, the sender accesses a secure environment – Evrotrust electronically signed specialized mobile application through which it is authenticated and submits the documents to be sent.

2. When using an API - Evrotrust first identifies the sender through its registration authority. After this identification, the sender uses cryptographic, session and API keys through which it is authenticated and submits the documents to be sent.

3. When using a web portal - Evrotrust uses a mobile application and performs initial identification of the sender through the video identification system certified as secure electronic identification within the meaning of Regulation (EU) No. 910/2014. By using two-factor identification, the sender accesses a secure environment - Evrotrust electronically signed specialized mobile application through which it is authenticated for access to and operation of the web portal through which it submits the documents to be sent.

Only after the successful authentication of the sender, the consignment is transferred from the system under its control to the QERDS system.

The authentication process takes place in a secure and controlled environment. All

evidence of the authentication and sending of the consignment is collected and stored in a protected environment.

4.5.2 IDENTIFICATION OF RECIPIENT

Evrotrust performs initial identification of the **recipient** in one of the following ways, depending on the user agent used:

1. When using a mobile application - the provider's registration authority first identifies the recipient through the video identification system certified as secure electronic identification within the meaning of Regulation (EU) No. 910/2014. By using two-factor identification, the recipient accesses a secure environment – Evrotrust electronically signed specialized mobile application through which it is authenticated and submits the documents to be sent.

2. When using an API - Evrotrust first identifies the recipient through its registration authority. After this identification, the recipient uses cryptographic, session and API keys through which it is authenticated and submits the documents to be sent.

3. When using a web portal - Evrotrust uses a mobile application and performs initial identification of the recipient through the video identification system certified as secure electronic identification within the meaning of Regulation (EU) No. 910/2014. By using two-factor identification, the recipient accesses a secure environment - Evrotrust electronically signed specialized mobile application through which it is authenticated for access to and operation of the web portal through which it submits the documents to be sent.

The evidence of receipt is provided as a separate electronic document in a strictly determined format, indicating the exact date and time of receipt of the user content by the recipient through a qualified time stamp. The evidence is electronically signed by the QERDS Certification Authority.

Only after the successful authentication of the recipient, the consignment is delivered by the QERDS system to the system under its control, and to the recipient respectively.

The authentication process takes place in a secure and controlled environment. All evidence of the authentication and receipt of the consignment is collected and stored in a protected environment.

4.6 EVIDENCE GENERATION

QERDS provides evidence of the sending and the receipt of user content.

Evrotrust collects and stores data on:

1. All events related to the initial verification of the identity of the sender and its identification;
2. All events related to the initial verification of the identity of the recipient and its identification;
3. At the initial verification of identity, the ID document data of a natural person (e.g. ID card or passport), identification data of a legal person (e.g. check in registers, powers of attorney, etc.) and all other data that are necessary for its correct determination are verified;
4. Data intended for initial identification of the sender/recipient;
5. Authentication level of the sender/recipient;
6. Evidence that the sender has been properly authenticated prior accepting the consignment;
7. Data on the operation of QERDS confirming the authentication of the sender and the recipient, as well as the communication between them;
8. Evidence that the user content has been received by the recipient;
9. Evidence that the user content has not been changed during the transmission.

4.6.1 EVIDENCE RELATED TO THE SENDER (S-ERDS)

Following the successful initial identification and authentication of the sender and the use of QERDS through S-ERDS, evidence of the sending is generated, which can also be provided to a third party. The evidence shows the exact date and time of sending the user content by the sender with a precise calibrated time against UTC (Coordinated Universal Time).

a. Submission Acceptance

The sender successfully transmits the user content to S-ERDS.

Evidence is generated with a presize date and time, indicating that the sender who was initially identified and properly authenticated has submitted a consignment to the ERDS system that has been accepted by the provider and the latter will take all necessary action to deliver it to the respective recipient(s).

b. Submission Rejection

The user content that has been sent to the S-ERDS by the sender has not been accepted by S-ERDS. The generated evidence shows that the sender who was initially identified and properly authenticated has transmitted the user content to the ERDS at a specific date and time, and that the ERDS system has refused to perform the necessary actions.

4.6.2 EVIDENCE RELATED TO THE RECIPIENT (R-ERDS)

Following the successful initial identification and authentication of the recipient and the use of QERDS through S-ERDS, evidence of the receipt is generated, which can also be provided to a third party. The evidence shows the exact date and time of sending the user content by the sender with a precise calibrated time against UTC (Coordinated Universal Time).

a. Evidence related to Content Consignment Delivery

The user content has been delivered to the recipient.

The related evidence shows that the consignment has been delivered to the recipient within the pre-set time after the recipient has been initially identified and properly authenticated.

b. Content Consignment Delivery Failure

The user content cannot be delivered to the recipient within a set period of time due to technical errors and/or for other reasons. There may be no evidence of delivery within the pre-set period of time.

The inability to deliver content may be caused by different events, such as:

- The ERDS system was unable to send the content from the sender to the recipient. In such a case, the evidence is generated by R-ERDS.
- While the message was in the ERDS system, no evidence of successful delivery has been received within a set period of time. In such a case, ERDS generates the evidence with the appropriate code of the reason for the failure to deliver.

4.6.3 EVIDENCE RELATED TO THE TRANSMISSION OF USER CONTENT TO THE RECIPIENT

a. Content Handover

The user content has successfully passed from R-ERDS to the recipient's application/user agent (UA). Events can be: pull (i.e. UA/the recipient's application automatically retrieves the user content from the R-ERDS - in recipients connected to API or through a portal) or push (the user content has been successfully delivered to the recipient's system by directly delivering the message to the recipient's system - mobile application, API or web portal).

The related evidence shows that the user content has been delivered at a specified date and time by the R-ERDS through UA/the recipient's application and upon its proper certification.

b. Content Handover Failure

The user content cannot be transmitted by the R-ERDS to the user agent (UA)/the recipient's application. In case of pull (i.e. the UA/the recipient's application automatically retrieves the message from the ERDS), the message cannot be downloaded within a given period due to technical errors and/or other reasons.

The related evidence shows that the content cannot be transmitted from the R-ERDS to the UA/the recipient's application after a certain number of attempts or a set waiting time. These parameters are specific and configured for the particular system.

4.7 PROTECTION OF THE TRANSMITTED DATA AGAINST THE RISK OF LOSS, THEFT, DAMAGE OR UNAUTHORIZED MODIFICATIONS

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

Confidentiality and integrity of data are important to the operation of Evrotrust and therefore cryptographic data protection techniques on removable media are used. To mitigate the risk of media aging, while the data stored is still needed, the data is transferred to new media before it becomes illegible. Evrotrust stores multiple copies of valuable data on different media to further reduce the risk of accidental damage or loss of data. The data communication is securely protected by an encrypted channel, thus eliminating the risk of loss, theft, damage or unauthorized modifications of data. The evidence is reliably stored to prevent against any

subsequent loss and theft in a protected environment under the control of Evrotrust for a period of 10 years.

4.8 TERMINATION OF SERVICE SUBSCRIPTION

The contract for the provision of a qualified electronic registered delivery service is terminated under one of the following circumstances:

a) closing a profile from the mobile application of Evrotrust with activation of the respective functionality. Termination is immediate;

b) other circumstances as outlined in "The Practice of Qualified Certification Services of Evrotrust.

Termination of the service is available 24 hours a day, 7 days a week. The time in the systems associated with the termination of a service contract for the provision of electronic registerd delivery service is synchronized to UTC at least every 24 hours.

4.9 TRUST STORAGE OF PRIVATE KEY

The private keys of the Evrotrust certification authority that are included in the Evrotrust certification hierarchy are personalized on portable holders and are not subject to trusted storage by Evrotrust.

The private keys of users who have requested certificates from a remote location via the Evrotrust mobile application are subject to trusted storage by Evrotrust and are stored in a Security Certified Module (HSM) encrypted for security level FIPS 140-2 Level 3.

5 CONTROL OF PHYSICAL AND ORGANIZATIONAL SECURITY

5.1 PHYSICAL SECURITY CONTROLS

The measures taken with regard 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 the ISO/IEC 27001 standard.

The measures related to the physical protection of information data, technology systems, premises and their related support systems are aimed at preventing:

- unauthorized access, damage and interference with working conditions;
- loss, damage or compromise of resources;

- compromise or theft of information or information processing tools.

The Evrotrust infrastructure is physically and logically distinct and is not used for any other activities performed by Evrotrust.

5.1.1 PREMISES AND PREMISES CONSTRUCTION

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

5.1.2 PHYSICAL ACCESS

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

Physical integrity is ensured for the equipment in the secure and isolated premise of Evrotrust. There is two-factor access control and 24-hour physical security. Physical access to critical equipment is not allowed for more than 30 (thirty) minutes per visit. Access to the cabinet holding the equipment is permitted to no less than 2 (two) authorized persons of Evrotrust. Every access to critical infrastructure premises is documented in special journals.

The protection of the Evrotrust building is realized by 24-hour security guards. There is an Alarm System, Video Surveillance System, Fire Alarm System and Access Control System in the premises of Evrotrust.

In Evrotrust, the offices of the Registration Authorities are detached and separated from the other premises. They are equipped with technique allowing for the safe storage of data and documents. Access to all areas is monitored and limited to authorized persons in accordance with their activities.

In the provider's buildings there are built systems for power supply and ventilation, flood and fire protection.

5.1.3 ACCESS CONTROL

Access to the Evrotrust system is limited to authorized persons:

- controls (such as firewalls) protect the internal network domains of Evrotrust against unauthorized access, including access by customers and third parties;

- the provider provides administrator access to operators, administrators and system auditors. The management manages user accounts, timely change or removal of access.
- access to the information and the system is limited in accordance with the division of trusted roles;
- Evrotrust employees are identified and certified before using critical service-related applications;

Evrotrust has taken measures to protect sensitive company data against disclosure and unauthorized access.

5.2 INCIDENT MANAGEMENT

Evrotrust classifies security incidents in two categories:

- those endangering the integrity of certification services (e.g. penetration or change of delivery location, system maintenance errors that endanger the integrity of systems/servers, physical access by unauthorized persons);
- those not endangering the integrity of certification services (e.g. loss of power supply, communication line failure, misuse of powers, attempts to penetrate the system).

If there is any doubt as to which category a security incident is classified in, the incident is considered to have been classified in the highest category.

Any person who witnesses or suspects a security incident is required to inform the management. Reporting security incidents may be performed in any way (personally, by telephone or email) that enables the relevant management persons to be notified as soon as possible.

The management is required to investigate the reported incident and to adopt or propose appropriate measures to prevent its recurrence.

Every security incident is recorded in a protocol.

Evrotrust implements procedures for notifying the relevant affected parties, in accordance with the applicable regulatory rules, of any security breach or loss of privacy that significantly affects the trust of the certification service provided and the personal data maintained therein, within 24 hours of identifying such breach. Where a security breach or loss of data may adversely affect a natural or legal person using the service, the provider will notify such person of the incident.

Evrotrust reviews every critical vulnerability within 48 hours of its identification.

5.3 STAFF CONTROL

Evrotrust ensures that its employees perform administrative and management procedures and procedures that are consistent with information security management, thereby ensuring the reliability and security of its operations.

Evrotrust recruits staff and, where applicable, hires subcontractors who have the necessary experience, reliability and qualifications and who have undergone training in security and protection of personal data.

Evrotrust applies appropriate disciplinary sanctions to employees who violate company policies or procedures.

Information security roles and responsibilities are documented in the job descriptions of the staff.

The management staff has the necessary experience and knowledge in relation to the QERDS service provided, they are familiar with the security and risk assessment procedures sufficient to perform their management functions.

The entire staff of the provider does not have any conflict of interest that could impair the impartiality of Evrotrust's business.

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

The subjects of activity examined during the audits for each of the standards are as follows:

- ISO 9001, ISO 22301- Provision of services related to electronic identification and services under Regulation (EC) No. 910/2014;
- ISO/IEC 27001– Information Security Management System for processing of personal

data of customers, corporate data and information systems for the provision of electronic identification and certification services in accordance with the Declaration of Feasibility version 1.0.;

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

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

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

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

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

5.5 ARCHIVING

Information about significant events is periodically archived in an electronic form.

Evrotrust archives all data and files related to: registration information; the system security; all requests submitted by customers; all customer information; all keys used by the Certification Authorities and the Registration Authority; and all correspondence between Evrotrust and its customers. All documents and data used in the identity verification process are subject to archiving.

The information under Art. Article 24 (2) (h) of Regulation (EU) No 910/2014 (all relevant information in relation to data issued and received by EVrotrust, in particular with a view to providing evidence in court proceedings and insurance of continuity in the provision of the service) is stored for a period of 10 years, including after the termination of the activity of EVrotrust.

The long-term storage of data is done in a secure and protected premise. The specific conditions are in line with the applicable standards, recommendations and regulations specified

in the field of information security.

Data is collected in a way consistent with the type of document.

Access to the long-term stored data is only allowed to authorized persons.

5.5.1 STORAGE OF DATA MEDIA

All media containing software, data repositories or audit information is safely stored in a special storage room with access control. There is a system of physical and logical protection in the Evrotrust storage room.

When data confidentiality or integrity is important for the operation of Evrotrust, cryptographic data protection techniques on removable media are used. To mitigate the risk of media aging, while the data stored is still needed, the data is transferred to new media before it becomes illegible.

Evrotrust could store multiple copies of valuable data on different media to further reduce the risk of accidental damage or loss of data.

5.5.2 WASTE DISPOSAL

Procedures for safe destruction of media have been put in place to minimize the risk of leakage of confidential information to unauthorized persons. The procedures for safe destruction of media containing confidential information are consistent with the sensitivity of such information.

Media containing confidential information are safely stored and destroyed by burning or cutting or deleting data when used by another application. Destruction of sensitive objects is recorded in a log in order to keep a history of the audit.

For damaged devices containing sensitive data, the risk is assessed of whether the objects should be physically destroyed or sent for repair.

Paper media containing significant Evrotrust security information will, after expiry of the storage period specified in the internal regulations, be destroyed in special cutting devices.

Information media containing cryptographic keys and their access codes used for their storage will be fragmented using suitable devices. This applies to media that do not allow for permanent deletion of stored data and its re-use.

In certain cases, information from portable media will be destroyed by deleting or

formatting the device without the possibility of recovery.

5.5.3 ASSET MANAGEMENT

Evrotrust ensures an adequate level of protection for its assets, including information assets. The provider maintains a list of all information assets and performs a risk assessment.

Evrotrust identifies the assets corresponding to the information life cycle and documents them by their level of importance. The information life cycle includes creation, processing, storage, exchange/transmission, deletion and destruction. The documentation is maintained in special inventories. The asset inventory is accurate, up-to-date and consistent.

Information is classified according to the regulatory requirements, its value, criticality and susceptibility to unauthorized disclosure or modification.

Asset handling procedures have been developed in accordance with the information classification scheme adopted by Evrotrust.

5.5.4 RECORDS OF EVENTS AND KEEPING LOGS

Evrotrust keeps records of:

- events related to the initial verification of the sender's identity and/or additional authentication;
- events related to the initial verification of the recipient's identity and/or additional authentication;

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

- events related to the sending and receipt of user content;
- security events, including security policy changes, system startup and shutdown, system failures and hardware failures, firewall and router and attempts to access the PKI system;
- the records related to the operation of the QERDS service are reliably and confidentially archived in accordance with the company's business practices;
- the exact time of significant events of key management and clock synchronization. The

system time is synchronized against UTC at least once every 24 hours;

- events are recorded in a way that does not allow for them to be easily deleted or destroyed;
- events having a significant impact on the security and reliability of the technology system, staff and customer control and impact on the security of the QERDS provided are recorded.

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

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

The information about the electronic journals is generated automatically.

Journals of records of registered events are stored in files for at least 6 (six) months. Throughout this period of time they are available online or in the process of searching by an authorized Evrotrust employee. After this period, the records are archived.

Archived journals are kept for a period of 10 (ten) years.

An archive is signed with an advanced electronic signature and qualified electronic time stamp. The log record information is periodically recorded on physical media stored in a special safe located in a premise with a high degree of physical protection and access control.

5.6 CHANGE OF KEYS

The Provider may change the Keys of the Certification authority "Evrotrust Services CA" and the Signatory "QERDS SU" in the case of:

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

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

- "QERDS SU", whose key is the signature of the evidence, and whose key will be changed, suspends the issuance of certificates 60 (sixty) days before the remaining period of validity of the private key is equal to the period of validity of the last signed proof;
- The "Evrotrust Services CA" Certification Authority, whose private key signs the QERDS 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.

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

5.7.1 BUSINESS CONTINUITY PLAN

The company has developed, documented, implemented and currently maintains control plans, procedures and mechanisms in line with the International Standard ISO 22301 to ensure the necessary level of business continuity and information security during adverse events.

Evrotrust ensures:

a) an adequate management structure in order to prepare, mitigate and respond to a disastrous event using staff having the necessary authority, experience and competence;

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

c) information security control mechanisms within the procedures and supporting systems and tools for business continuity and recovery after a disaster;

d) compensating mechanisms for control of the information security control mechanisms that cannot be maintained during an adverse event.

A business continuity plan is provided that involves duplication of critical systems. Backup is stored in geographically remote locations. The specific conditions are in line with the applicable standards, recommendations and regulations specified in the area of information security.

The company reviews at regular intervals of time the mechanisms created for control of the information security continuity so as to ensure their effectiveness and efficiency during adverse events.

Evrotrust regularly creates backups of important information and software and ensures that all basic information and software can be recovered after a disaster or in case of loss of the archive.

Recovery mechanisms are reviewed regularly to ensure that they meet the requirements of the Business Continuity Plan.

The provider's database necessary to restore QERDS activity in the event of an incident or a disaster is maintained and stored in safe and secure locations. Evrotrust has the obligation to inform senders, recipients and third parties upon the occurrence of any incidents in the service provision activities.

5.8 TERMINATION OF THE ACTIVITY OF A CERTIFYING AUTHORITY

Before the certifying authority terminates its services "Evrotrust Services CA", it is required to:

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

- makes reasonable commercial efforts to minimize distortion of consumer interests.

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

6 CONTROLS OF TECHNICAL SECURITY

6.1 GENERATION AND INSTALLATION OF KEY PAIRS

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

6.2 PROTECTION OF PRIVATE KEYS AND CRYPTOGRAPHIC MODULE

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

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

QERDSP uses advanced protocols and algorithms to encrypt the transmitted data.

6.3 OTHER ASPECTS OF THE MANAGEMENT OF KEY PAIRS

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

6.4 ACTIVATION DATA

The procedure for activation of key pairs of the Evrotrust Services CA and the signatory of QERDS

SU follows the procedures described in paragraph 6.2 of the document "Practice of Qualified Certification Services."

6.5 COMPUTER SECURITY

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

6.6 SECURITY OF THE TECHNOLOGY SYSTEM LIFE CYCLE

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

6.6.1 INFORMATION SYSTEM VULNERABILITY ASSESSMENT

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

The analysis of the activities and the supervision of the performance of all procedures are regularly performed by authorized persons of Evrotrust or automatically by the security systems of all information and communication devices of Evrotrust. The vulnerability assessment is based on analysis of logs, security events, and other important data.

6.7 NETWORK SECURITY

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

7 PROFILES OF QUALIFIED CERTIFICATES, CRL AND OF OCSP

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 “)

„Evrotrust Services CA“ with OID: 1.3.6.1.4.1.47272.2.14 is a Certification Authority of the qualified electronic registered delivery service that certifies the generated evidences according to this policy.

Version	V3	
Serial number	38 00 00 00 07 58 f6 72 2b 87 3d 45 0d 00 00 00 00 00 07	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Root CA
	OU=	Evrotrust Qualified Root Authority
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	10 July 2019, 12:50:59 UTC	
Validit to	10 July 2029, 13:00:59 UTC	
Subject	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Public Key Type/Length	RSA (4096 Bits)	
Subject Key Identifier	1b 3a 9e 6d 31 91 a1 5b 46 19 84 fe 9c 98 60 2c 09 d3 33 2e	
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSARootCA.crl	
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://ca.evrotrust.com/aia/EvrotrustRSARootCA.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca.evrotrust.com/ocsp	
Subject Alternative	RFC822 Name=servicesca@evrotrust.com	

Name	URL=http://www.evrotrust.com
Authority Key Identifier	KeyID=74 5c a1 40 73 2e 1f e6 f9 3b bc ab a0 a4 a7 54 44 74 4f 70
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constrains (critical)	Subject Type=CA Path Length Constraint=0

Thumbprint (SHA1): 7448b95dc14ff7127af731c580e0d6ca74f3fe10

Thumbprint (SHA256):

5c7ac0f5ada82e251b4cb8d701a43a4a5baf369289d4f29e27ab2690a88162ec

7.3 PROFILE OF CERTIFICATE STATUS AUTHORITY „EVROTRUST SERVICES VALIDATION"

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

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

<table>
<tr><td></td><td colspan="2">[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>Authority Key Identifier</td><td colspan="2">KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E</td></tr>
<tr><td>CRL Distribution Points</td><td colspan="2">[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://services.evrotrust.com/EvrotrustServicesCA.crl</td></tr>
<tr><td>Authority Information Access</td><td colspan="2">[1]Authority Info Access
Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
Alternative Name:
URL=http://services.evrotrust.com/EvrotrustServicesCA.crt
[2]Authority Info Access
Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name:
URL=http://services.evrotrust.com/ocsp</td></tr>
<tr><td>Basic Constraints (critical)</td><td colspan="2">Subject Type=End Entity
Path Length Constraint=None</td></tr>
<tr><td rowspan="5">QCStatements</td><td>id-qcs-pkixQCSyntax-v2[i] (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-SemanticsId-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>

Thumbprint SHA1: E1CBEE3169AE35A4E3C842B91A962F1B9DD8BFA3

Thumbprint SHA256:

95D9B9BDDF5CD372E84E02AC52A38592ADE3453DC5CE0904AE75E8CA35227705

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

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

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

7.5 PROFILE OF „EVROTRUST QERDS SU“

"Evrotrust QERDS SU 2024" is a qualified certificate for the qualified registered delivery service. It electronically signs the evidences using a signing unit (SU) that are issued under this policy. The qualified certificate of "Evrotrust QREMS SU" is:

Version	V3	
Serial number	4E70FB9EC7F53BEDD0429638EF9A7B1E0837FF1C	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust Services CA
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Valid from	Jan 18 07:14:25 2024 GMT	
Validit to	Jan 16 07:14:24 2029 GMT	
Subject	CN=	Evrotrust QERDS SU 2024
	organizationIdentifier	NTRBG-203397356
	O=	Evrotrust Technologies JSC
	C=	BG
Public Key Type/Length	RSA (2048 Bits)	
Authority Key Identifier	KEYID=1B3A9E6D3191A15B461984FE9C98602C09D3332E	
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>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.10.1
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</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>3CCF5B8E6887A70A1F59C4EA65D8A8FD445D8ABD</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): B13F7EE4471C07F55C2DF369A81A14A99EB86F3A

Thumbprint (SHA256):

3371CFA10C7312A51A6562F7EE827913726444D5147C37F79D7E35CC9A4A3403

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.

9.5.4 TRUSTED ROLES CARE

The trusted roles should pay due care, as described in paragraph 9.6.4 of the document "Practice of Qualified Certification Services".

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.