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

CERTIFICATE POLICY AND PRACTICE FOR PROVIDING A REGISTRATION AUTHORITY QUALIFIED SERVICE FOR IDENTIFICATION AND VERIFICATION OF SPECIFIC ATTRIBUTES FOR ISSUING A CERTIFICATE BY PHYSICAL PRESENCE

CONTENTS

1 INTRODUCTION 3
1.1 OVERVIEW 3
1.2 COMPLIANCE 4
1.3 POLICY NAME AND IDENTIFIER 5
1.4 POLICY MANAGEMENT 5
2 DEFINITIONS 5
3 REGISTRATION AUTHORITY 8
4 OPERATING ACTIVITIES OF THE REGISTRATION AUTHORITY 9
4.1 ESTABLISHING A NATURAL PERSON'S IDENTITY 10
4.2 VERIFICATION OF A LEGAL PERSON'S IDENTITY 11
4.3 ESTABLISHING THE IDENTITY OF A NATURAL PERSON WHICH ACTS AS A REPRESENTATIVE OF A LEGAL PERSON 12
5 USE AND APPLICABILITY OF THE RA IDENTIFICATION SERVICE 14
6 REPOSITORY 14
7 CONTROL OVER THE PHYSICAL SECURITY OF THE RA PREMISES 14
7.1 THE PHYSICAL ACCESS 14
7.2 ELECTRICAL SUPPLY AND CLIMATIC CONDITIONS 15
7.3 FLOODING 15
7.4 FIRE PREVENTION AND FIRE PROTECTION 15
8 ORGANIZATIONAL CONTROL 15
9 CONTROL AND TRAINING REQUIREMENTS FOR THE RA OPERATORS 16
9.1 CONTROL OVER THE RA OPERATORS 16
9.2 STAFF QUALIFICATION 16
9.3 PROCEDURES FOR STAFF VERIFICATION 17
9.4 TRAINING REQUIREMENTS FOR THE STAFF OF THE RA OF EVROTRUST 17
9.5 TRAINING FREQUENCY AND REQUIREMENTS FOR QUALIFICATION UPGRADE FOR THE EMPLOYEES OF THE RA 18
9.6 PENALTIES FOR UNAUTHORIZED ACTIONS TAKEN BY THE EMPLOYEES OF RA 18
10 ACTIONS IN THE EVENT OF ACCIDENTS 18
11 CONTINUITY OF THE SERVICE AND RECOVERY AFTER ACCIDENTS 19
12 COMPUTER SYSTEMS SECURITY 19
13 VERIFICATION AND CONTROL OVER THE ACTIVITY OF THE RA 20
13.1 INTERNAL AUDITS 20
13.2 INDEPENDENT EXTERNAL AUDIT 20
13.3 VERIFICATION BY THE NATIONAL SUPERVISORY BODY 21
14 FINANCIAL RESPONSIBILITIES 21
15 INSURANCE OF ACTIVITY 21
16 INVIOLABILITY OF PERSONAL DATA 21
17 LIABILITIES, RESPONSIBILITY AND GUARANTEES OF THE REGISTRATION AUTHORITY 22
18 DISCLAIMER 22

1 INTRODUCTION

"Certificate Policy and Practice for Providing a Registration Authority Qualified Service for Identification and Verification of Specific Attributes for Issuing a Certificate by Physical Presence" (the Policy/CP-CPS-RA-P/Certificate policy and practice for providing Registration authority qualified service for identification and verification of specific attributes for issuing a certificate via physical presence) is a document describing the general rules, requirements, procedures and scope of applicability used by Evrotrust for providing a registration service which verifies natural and legal persons' identity and, if applicable, specific attributes related to those persons.

The service is provided for trust service providers (providers, TSPs) - clients of Evrotrust. The natural and legal persons subject to identification and verification of specific attributes are users of such TSPs. As a result from the verification of identity performed by a Registration Authority of Evrotrust, the TSP provides trust services and issues certificates for electronic signatures/seals. The verification is performed by means of physical presence of the persons who are users of TSPs, at an office of the Registration Authority ("the RA") of Evrotrust. The Registration Authority may be an internal structure of Evrotrust or a subcontractor acting as an external Registration Authority to whom Evrotrust has assigned the registration activity as a whole or in parts, by virtue of contractual relations.

The Registration Authority qualified service of Evrotrust, which is furnished in accordance with this Policy and Practice, may be provided as a service to clients (other TSPs) in compliance with Regulation (EU) No 910/2014. The relations between Evrotrust and the other TSPs are settled by virtue of a contract for service provision.

1.1 OVERVIEW

Evrotrust, in its capacity as a trust service provider, provides an RA service of estabishing identity by means of physical presence of TSP users, in compliance with Regulation (EU) No 910/2014, by applying procedures which ensure high level of reliability and security of the verified information identifying the users. Evrotrust applies procedures which ensure reliability and security during confirmation of the identification status of a particular person. The RA service is a

major part of the activities of each TSP and the TSP applies adequate measures ensuring reliability and security while issuing certificates and the related cryptographic keys. The relations between Evrotrust that provides the RA service and the TSPs which are clients of the service are settled by virtue of a contract.

1.2 COMPLIANCE

Evrotrust provides a Registration Authority qualified service for identification by physical presence covering the requirements of item 5.5.1.3 (a) of TS 119.612 Trusted Lists. In this sense, Evrotrust defines the service on a national level as of the type: URI: http://uri.etsi.org/TrstSvc/Svctype/RA.

The Policy complies 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 (Regulation (EU) No 910/2014), and with the applicable laws in the Republic of Bulgaria;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protecion Regulation);
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 General requirements;
- TS 119 612 Trusted Lists.

The activities of Evrotrust related to the provision of this service have already been verified by an independent verification entity in accordance with Regulation (EU) 910/2014 for the purposes of the company's own activity as a qualified trust service provider, and Evrotrust has been entered in the national Trusted List kept by the Communications Regulation Commission. The service shall therefore be considered a qualified one.

1.3 POLICY NAME AND IDENTIFIER

The name of this document is: "Policy and Practice for Providing a Registration Authority Qualified Service for Identification and Verification of Specific Attributes for Issuing a Certificate by Physical Presence", with object identifier/OID: 1.3.6.1.4.1.47272.2.16.17.1.1.

1.4 POLICY MANAGEMENT

The Management Body of Evrotrust is responsible for managing the Policy.

The Policy is a public document. It may be altered by Evrotrust at any time, each new revision being notified to the interested parties by publishing it on the Evrotrust website. https://www.evrotrust.com/landing/bg/a/tsp-documents.

Each version of the Policy shall be in force until a new version is approved and published. Each new version shall be developed by authorized competent employees of Evrotrust and it shall be published following an approval by the Board of Directors of Evrotrust.

The contact person for the purposes of managing the document "Policy and Practice for Providing a Registration Authority Qualified Service for Identification and Verification of Specific Attributes for Issuing a Certificate by Physical Presence", shall be the CEO of Evrotrust.

Additional information may be received at the following address:

Evrotrust Technologies AD

Sofia, 1766

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

phone, fax: + 359 2 448 58 58

e-mail: office@evrotrust.com

2 DEFINITIONS

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

"Signatory" means a natural person who creates an electronic signature;

"**Electronic signature**" means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

"**Advanced electronic signature**" means an electronic signature which meets the requirements set out in Regulation (EU) No 910/2014;

"**Qualified electronic signature**" means an advanced electronic signature that is created by a qualified electronic signature creation device and which is based on a qualified certificate for electronic signatures;

"**Electronic signature creation data**" means unique data which is used by the signatory to create an electronic signature;

"Certificate for electronic signature" means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;

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

"Trust service" means an electronic service normally provided for remuneration, which consists of:

a) the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or

b) the creation, verification and validation of certificates for website authentication; or

c) the preservation of electronic signatures, seals or certificates related to those services;

"**Qualified trust service**" means a trust service that meets the applicable requirements laid down in Regulation (EU) No 910/2014;

"**Qualified trust service provider**" means a trust service provider who provides one or more qualified trust services and is granted the qualified status by a supervisory body;

"**Creator of a seal**" means a legal person who creates an electronic seal;

"**Electronic seal**" means data in electronic form which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

"**Advanced electronic seal**" means an electronic seal which meets the requirements set out in Regulation (EU) No 910/2014;

"**Qualified electronic seal**" means an advanced electronic seal, which is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seal;

"**Electronic seal creation data**" means unique data, which is used by the creator of the electronic seal to create an electronic seal;

"Certificate for electronic seal" means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;

"Qualified certificate for electronic seal" means a certificate for an electronic seal, which is issued by a qualified trust service provider and meets the requirements laid down in Regulation (EU) No 910/2014;

"**Electronic time stamp**" means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

"**Qualified electronic time stamp**" means an electronic time stamp which meets the requirements laid down in Regulation (EU) No 910/2014;

"**Electronic document**" means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

3 REGISTRATION AUTHORITY

Before the process whereby a TSP issues a qualified certificate, the RA, by appropriate means and complying to the national laws, has to verify the identity and, if applicable, all specific attributes for the natural or legal person to whom a qualified certificate is issued. The RA performs an authenticity service only for the identification data which is appropriate, significant, and does not exceed what is necessary for a trust service to be received. The RA observes that the requirements for legal processing of personal data are met in accordance with GDPR, and with regard to the confidentiality and security of the processing activities. The RA has qualified persons with the necessary expert knowledge, trustworthiness, experience and qualification, who have undergone appropriate training in the rules of security and personal data protection, and it applies administrative and management procedures that comply with the European or international standards.

The RA carries out primarily, but not only, the following activities:

- It accepts requests for issuing certificates, approves or rejects such requests in accordance with the adopted internal rules for approval;
- It establishes the identity of the persons who have submitted requests for issuing certificates;
- It confirms the identification of the persons by means of verification and makes their registration by entering them in the TSP's database.

Contact information of the Registered Authorities of Evrotrust is available on the Internet page of Evrotrust: https://www.evrotrust.com/landing/bg.

The RA is an internal structure of Evrotrust and/or subcontractor of Evrotrust (natural or legal person to whom Evrotrust assigns to carry out activities for providing an RA service), which

is responsible for identifying the holders of qualified certificates and the users of trust services who are customers of Evrotrust clients (TSPs). The RA supports the process of request submission for issuing a qualified certificate and using TSP services. The RA carries out its activities at an office of Evrotrust, the location of which is announced on the Internet page of the TSP. Evrotrust may assign to subcontractors (an external RA), or be responsible for the activity as a whole, or for parts of it, for identification of the holders of qualified certificates and users of TSP trust services.

4 OPERATING ACTIVITIES OF THE REGISTRATION AUTHORITY

When the person makes a first visit to an office of the RA and requests that a trust service be provided to him/her, the operators implement procedures which enable, before issuing a qualified certificate or providing a trust service, data to be collected on the person's identity and that same person to be identified in compliance with Art. 24, par. 1 of Regulation (EU) No 910/2014. The collected and verified information is included in the certificates. At the stage of registration of the TSP user, a mandatory verification of the provided data is performed, thus guaranteeing that the information contained is accurate and true at the moment of issuing the certificates.

Evrotrust guarantees that the natural and legal persons have been identified correctly, that their identity has been verified, and that the requests for providing an identification service, for issuing qualified certificates and/or providing other trust services are fully, accurately and duly verified and approved, the full name and legal status of the respective natural/legal person and the relation between the verified data and the natural/legal person included.

A registration account is created for each person in the TSP systems, containing data on his/her identity and saved in the provider's database. The registration account contains the minimum set of data required for user identification, a consent for key pair generation and issuance of a qualified certificate. The certificate issued by the TSP contains verified data from the identity document; in specific cases, however, it might contain additional attributes beyond the mandatory ones for a qualified certificate which arise from Art. 28, item 3, and Art. 38, item 3 of Regulation (EU) No 910/2014.

Personal data are processed in a way that guarantees high level of security, including

protection against unauthorized or illegal processing, and against accidental loss, destruction or damage, by applying appropriate technical and organizational measures (integrity and confidentiality).

4.1 ESTABLISHING A NATURAL PERSON'S IDENTITY

Verification of a natural person's identity is performed on-site, at an office of the RA, by an operator of the RA verifying an identity document. For the purposes of identification, the person shall provide a valid identity document to the RA operator.

The operator performs identification by comparing the document photo with the person physically present. The data from the identity document may be verified in primary registers of the identity documents of the population and others, or by automatically extracting data from documents with contact or contactless interface (via NFC, for example). After identification and verification of the validity of the data from the identity document , the RA creates an account of the person in the TSP system. A server generates a document for performed identification of the person, and a request for issuing a qualified certificate is sent to the certifying authority of the TSP.

The minimum set of natural person's personal data has to include different scope of data, for example:

a) family name or names;

b) given name or names;

c) date of birth;

d) unique national identifier, if available, in accordance with the technical specifications for the purposes of cross-border identification, the identifier remaining unchanged for as long as possible; for the Republic of Bulgaria an example is the Personal number [EGN]/Personal number of a foreigner.

The set of natural person's data may have additional specific attributes on one or more of the following items:

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

b) place of birth;

c) permanent address;

d) sex;

e) mobile phone number;

f) e-mail address;

g) others (the provider may, depending on the implemented integration with the different types of identity documents, with primary registers and reliable data sources, add to the set of specific attributes).

The person's personal data may be entered automatically in the provider's system after scanning the identity document. In this case, the provider shall not store the scanned copy of the document, unless its user requests that, in compliance with the requirements of the General Data Protection Regulation (GDPR).

The RA verifies the information authenticity, by all legally permitted means, in the respective primary registers and reliable data sources. The RA operator verifies the session by an electronic signature the fact that he/she has verified the person's identity on the basis of physical presence.

The RA suspends the identification process if, while the verification is in progress, it is found out that the person:

a) has been placed under judicial disability;

b) has provided untrue data for the registration;

c) has declared a change in already verified information, on the basis of which the registration has been performed.

TSP users have the opportunity to suspend their account by physical presence at an office of an RA of Evrotrust, by e-mail, by phone, or in any other way which has been agreed upon.

4.2 VERIFICATION OF A LEGAL PERSON'S IDENTITY

Establishing a legal person's identity is subject to verification on the basis of documents presented before an RA operator, or by verification in reliable sources (in the Republic of Bulgaria, for example, verification is performed in the respective registers, by using the UIC [Unified Identification Code], BULSTAT respectively, which has been provided, pursuant to the E-Governance Act). The verification may be automated.

The minimum set of data for a legal person may consist of the data specified below:

a) legal name (company name);

d) unique national identifier, in accordance with the technical specifications for the purposes of cross-border identification, the identifier remaining unchanged for as long as possible (for the Republic of Bulgaria an example is the UIC/BULSTAT).

The set of legal person's data may consist of additional specific attributes on one or more of the following items:

a) management address;

b) VAT registration number, when it is different from the unique national identifier;

c) tax number, if it is different from the unique national identifier or the VAT number;

d) identification code in accordance with Article 3, paragraph 1 of Directive 2009/101/EC of the European Parliament and of the Council (1);

e) legal entity identifier (LEI), as stipulated in Commision Implementing Regulation (EU) No 1247/2012 (2);

e) economic operator identification number (EORI number), as stipulated in Commision Implementing Regulation (EU) No 1352/2013 (3);

f) excise number, provided for in Article 2, paragraph 12 of Council Regulation No 389/2012 (4);

g) others (the provider may, depending on the implemented integration with the different types of identity documents, with primary registers and reliable data sources, add to the set of specific attributes).

Evrotrust should take measures to minimize the risk of the legal person's identity not corresponding to the declared one. Evrotrust should verify the information authenticity by all legally permitted means in the respective public registers and reliable sources. The RA shall suspend the identification process if, during the verification, it finds out that the legal person has been placed under judicial disability and/or has provided untrue data for the registration. The operator shall suspend the identification process in the event of any change in already verified information, on the basis of which the registration has been performed.

4.3 ESTABLISHING THE IDENTITY OF A NATURAL PERSON WHICH ACTS AS A

REPRESENTATIVE OF A LEGAL PERSON

For establishing the identity of a natural person who is a representative of a legal person (managers, board members, authorized agents, etc.), when representative power is granted by operation of law, verification of a registration document which gives rise to legal representative power (Certificate of Current Status, etc), or verification in publicly accessible registers (in Bulgaria, for example, verification is performed in the registers of the Registry Agency) is performed. The verification is performed on the basis of unique national identifier which remains unchanged for as long as possible (in the Republic of Bulgaria, for example, this is the UIC/BULSTAT), or by other specific attributes. For natural persons, an identity verification is performed pursuant to item 4.1 of the previous section.

For establishing the identity of a natural person who is a representative of a legal person by virtue of authorization, the RA operator performs verification of documents pursuant to item 4.1 and item 4.2, an empowerment order, a power of attorney certified by a notary, or electronic empowerment with a qualified electronic signature. The verification may be automated.

The legal person's identity verification performed by the RA of Evrotrust aims at proving that, during consideration of the request for the TSP to issue a qualified certificate, the legal person is existing and that the representing or authorized person that applies for a qualified certificate has representative powers or a power of attorney to request the issuance.

During verification, the operator may suspend the process of issuing a qualified certificate if he/she finds out that:

a) the natural person who is a representative of the legal person has been placed under judicial disability or has not reached the age of majority;

b) the representative powers of the natural person with regard to the legal person have been terminated;

c) untrue data has been provided for the registration of a natural person who is a representative of a legal person;

d) the legal person has been declared insolvent;

e) upon a change in already verified information, on the basis of which the registration has been performed.

5 USE AND APPLICABILITY OF THE RA IDENTIFICATION SERVICE

The RA identification and persons' identity authentication service provided by Evrotrust is available for Evrotrust clients (TSPs) and relying parties from the private and the public sector in the Republic of Bulgaria, as well as in countries beyond its territory.

6 REPOSITORY

The TSP records and stores the information related to the process of identification and qualified certificate management, in accordance with the applicable laws and the good practices regarding data protection and retention.

7 CONTROL OVER THE PHYSICAL SECURITY OF THE RA PREMISES

The measures which are taken for physically protecting the RA and Evrotrust are an element of the Information Security System developed and implemented in Evrotrust and complying to the requirements of the ISO/IEC 27001, ISO 9001, ISO 22301 and ISO/IEC 20000-1 standards. The measures taken with regard to the physical protection of the information data, of the technological systems, the premises and the supporting systems related to them, are directed towards prevention of:

- unauthorized access, damages and intervention in the working conditions;
- loss, harm, or undermined resources;
- undermining or stealing information, or information processing means.

7.1 THE PHYSICAL ACCESS

The offices of the RA of Evrotrust are set apart and separated from the other premises. Technical equipment is installed in them, allowing for safe storage of data and documents. Access to these zones is monitored and limited only to authorized persons associated with the

Registration Authority activities (Registration Authority operators, system administrators), authorized employees of clients and of TSP users.

7.2 ELECTRICAL SUPPLY AND CLIMATIC CONDITIONS

Evrotrust technological systems are powered by two independent UPS systems.

External electrical feed by a diesel generator is maintained as reserve. In the event of a breakdown in the main power line, the system switches to an emergency source of electrical power (UPS and/or electrical energy). The working environment in the computer systems area is monitored constantly and independently from the other working environments. The RA is connected to the emergency energy system of the central building of Evrotrust.

7.3 FLOODING

For moisture monitoring in the computer systems premises, as well as in the whole territory of the building of Evrotrust, moisture level reading sensors have been installed. These sensors have been integrated in the security system of the building of Evrotrust. The security guards and empolyees of Evrotrust have been instructed and are obliged, upon occurrence of any potential threats, to immediately notify the respective authorities, the security administrator and the system administrator.

7.4 FIRE PREVENTION AND FIRE PROTECTION

Evrotrust complies with all fire safety rules by carrying out its activities in compliance with all normative and standardisation requirements in this field.

8 ORGANIZATIONAL CONTROL

All procedures concerning the security when providing an RA service of identification and verification of specific attributes for the issuance, administration and use of qualified certificates

for electronic signature are implemented by trusted staff of Evrotrust. Evrotrust keeps sufficient number of qualified employees so that, at any time during performance of its activities, such employees can ensure compliance with the legislation which is in force and with the internal rules and regulations of Evrotrust.

9 CONTROL AND TRAINING REQUIREMENTS FOR THE RA OPERATORS

9.1 CONTROL OVER THE RA OPERATORS

The staff of Evrotrust that performs activities in the RA consists of sufficient number of highly qualified employees. The persons performing operator's activities have appropriate professional training and experience, which guarantees that security requirements during the identification of TSP users are met. The employees of Evrotrust undergo periodic continuing training courses, which meet the contemporary requirements within the field of the provided activities.

9.2 STAFF QUALIFICATION

Evrotrust ensures that the person working in the RA system meets at least the following requirements for taking up the position:

- he/she has at least secondary education completed (inasmuch as there are no other requirements for the respective position);
- he/she has signed a part-time or full-time contract where his/her role within the system and the respective responsibilities are described;
- he/she has undergone appropriate training related to the scope of obligations and tasks for his/her position;
- he/she has received training in the field of personal data protection;
- he/she has signed an agreement with a clause concerning the protection of sensitive (from the point of view of TSP security) information and confidentiality of users' data;
- he/she does not perform tasks which might lead to conflict of interests with the activities of Evrotrust.

9.3 PROCEDURES FOR STAFF VERIFICATION

Each new employee at the RA is verified by Evrotrust:

- to confirm his/her previous employment;
- to verify his/her recommendations;
- to confirm his/her degree of education;
- to verify his/her conviction status certificate;
- to verify his/her identity document;
- etc.

In case that the required information is not available (due to any law which is in force, for example), Evrotrust uses other legally permitted methods which allow collection of the necessary information.

Evrotrust may reject the application in relation to the performance of this activity, if it finds out that:

- it has been mislead by an applicant with regard to the required data specified above;
- it gets highly unfavourable or not very reliable recommendations from previous employers;
- information is received that the applicant has criminal record, or that he/she has been sentenced by virtue of a valid court ruling which has entered into force.

In case that any of the hypotheses above exists, further steps shall be taken in compliance with the safety procedures of Evrotrust and the applicable laws.

9.4 TRAINING REQUIREMENTS FOR THE STAFF OF THE RA OF EVROTRUST

The staff that performs functions and tasks resulting from their employment with the RA must undergo the following trainings:

- regulations, procedures and documentation related to the position;
- security technologies and security-related procedures used by the RA;
- personal data protection (GDPR);

- system software of the RA;
- responsibilities arising from tasks performed within the system.

9.5 TRAINING FREQUENCY AND REQUIREMENTS FOR QUALIFICATION UPGRADE FOR THE EMPLOYEES OF THE RA

Evrotrust provides regular trainings to the RA employees. These trainings are subject to additions upon any change in the national legislation, within the sector, or upon any change in the documentation and activities of Evrotrust.

9.6 PENALTIES FOR UNAUTHORIZED ACTIONS TAKEN BY THE EMPLOYEES OF RA

In the event of established or suspected unauthorized access, the system administrator may suspend the perpetrator's access to the RA system. Further disciplinary actions shall be consulted with the Management of Evrotrust.

10 ACTIONS IN THE EVENT OF ACCIDENTS

For actions that should be taken in the event of any accidents in the activities of the RA, Evrotrust has developed and Emergency Plan, which is reviewed once a year. Evrotrust must be able to find out each possible incident. Following an analysis of the situation, the objective is to prevent future incidents based on system errors or on breakdowns in services or technologies. In order for al this to happen, Evrotrust constantly monitors all systems and services (24x7x365).

The Plan indicates the approximate time for detecting any type of incidents. Evrotrust guarantees that each potential incident can be found out. Evrotrust is able to differentiate a real incident from a false alarm. Grave incidents are reported to the Management of Evrotrust and to the provider. The Plan indicates the approximate time for notification and confirmation. It defines roles and responsibilities. It provides assessment of the type of incident, the appropriate reaction time and the actions which shall follow. The events are recorded. The reasons for the incident are documented, as well as the way in which it has influenced work efficiency. The measures taken

are recorded (reaction time and time for service and system recovery, etc.). Improvements are proposed.

In the event of any breakdowns in the hardware, software, or in the data, Evrotrust notifies the client (TSP), restores the components of the infrastructure and makes a priority of recovering the access to the service. For such cases, Evrotrust has developed an Emergency Plan. Evrotrust has a plan for management of all incidents which affect normal functioning of the service. This plan is in accordance with a Business Plan, a Continuity Plan and a Disaster Recovery Plan.

11 CONTINUITY OF THE SERVICE AND RECOVERY AFTER ACCIDENTS

Evrotrust has developed a Service Continuity Plan for the cases when accidents occur, such as major system or networks interruptions. The objective is to achieve continuity in the RA activities and to protect the business when there are major interruptions of normal business operations.

The Security Policy followed by Evrotrust takes into account the following threats affecting the continuity of the provided service:

- breakdown in the computer system of Evrotrust, including breakdown in network resources - may happen accidentally;
- breakdown in the software, any fault or suspension of the access to data - may happen through inappropriate applications or malicious software;
- loss of important network services related to the RA activities - may happen upon a breakdown in the electrical grid;
- undermining part of the network used by Evrotrust for provision of the RA service.

The procedures for system recovery after accidents are tested upon each component of the technological system of Evrotrust at least once a year. These tests are part of the internal audit.

12 COMPUTER SYSTEMS SECURITY

The procedure is described in item 6.6. of the document "Certification Practice for Providing Qualified Trust Services".

13 VERIFICATION AND CONTROL OVER THE ACTIVITY OF THE RA

13.1 INTERNAL AUDITS

The purpose of the internal audits of the activities of the RA is to control the provision of trust services and identification activity, inasmuch as it is compatible with the integrated management system which is implemented and which includes the requirements of the ISO/IEC 27001, ISO 9001, ISO 22301, and ISO/IEC 20000-1 standards, and of Regulation (EU) No 910/2014, Regulation (EU) 2016/679, as well as the internal management decisions and measures. The audits which are performed refer to the internal as well to the external RAs (subcontractors of Evrotrust). The RAs are subject to at least one internal audit annually. The results from the audits are summarized in reports. Based on the assessments made in the report, the Management of Evrotrust plans measures and deadlines for removal of the omissions and incompliances which have been found. The clients of Evrotrust, upon their request, are provided with access to the reports.

13.2 INDEPENDENT EXTERNAL AUDIT

As a main structure of Evrotrust and part of the infrastructure of Evrotrust as a qualified trust service provider, the RA is subject to an audit at least once every 24 months by a Conformity Assessment Body which audits the activities of Evrotrust as a whole. The audit confirms that Evrotrust and the RA with the identification service provided by it in particular, meet the requirements set out in Regulation (EU) No 910/2014.

The RA activities are included in an audit at least once every 36 month by an independent verification team concerning the international standards ISO/IEC 27001, ISO 9001, ISO 22301, ISO/IEC 20000-1. The purpose of the audit is to confirm that the RA activities are compatible with the implemented integrated management system.

13.3 VERIFICATION BY THE NATIONAL SUPERVISORY BODY

The National Supervisory Body may, at any time, carry out a verification, or request that a Conformity Assessment Body perform an audit for assessment of the conformity of the activities of Evrotrust, and of the RA in particular, with the requirements of Regulation (EU) No 910/2014 and the national legislation.

14 FINANCIAL RESPONSIBILITIES

Evrotrust is responsible for the provided service to the clients (TSP) that rely on the identification of their users. Evrotrust is liable if damages are due to its fault, or to the fault of the parties to whom it has assigned the identification activity. If Evrotrust acknowledges and accepts that damages have occurred, it undertakes to pay such damages which are a direct and immediate consequence of the negligence of RA operators.

15 INSURANCE OF ACTIVITY

Evrotrust takes out a compulsory insurance of its activities, which shall also include its activity on providing identification service to the RA. Evrotrust is liable for intentional damages, or damages that have been negligently caused to a natural or a legal person because of the RA's operators failure to fulfil their obligations.

16 INVIOLABILITY OF PERSONAL DATA

Evrotrust is a Personal Data Administrator pursuant to the Personal Data Protection Act and GDPR. In its capacity as Personal Data Administrator, it strictly observes the meeting of the requirements for confidentiality and non-distribution of personal data of persons that became known during the performance of the identification activity by the PO operators.

17 LIABILITIES, RESPONSIBILITY AND GUARANTEES OF THE REGISTRATION AUTHORITY

Evrotrust guarantees that the RA fulfills its functions and obligations in full compliance with the terms and conditions of this document and with the company's operational instructions. Evrotrust is responsible for the actions of its RA, that:

- it carries out its activities using reliable and secure devices and software;
- it provides a service which complies with the national legislation;
- it makes the necessary efforts to perform correct person identification, it enters the data in a correct and accurate manner in the provider's database, and updates this information at the moment of data confirmation;
- it does not make intentional mistakes or enter inaccuracies in the information contained in the qualified certificates.

18 DISCLAIMER

Evrotrust shall not be liable in case of damages caused by:

- illegal actions taken by users and providers;
- accidental events characterized as force majeure, including malicious actions of third parties.

This document is published on the website of Evrotrust in Bulgarian and English. In the event of any discrepancy between the texts in Bulgarian and English, the Bulgarian text shall prevail.