evrotrust
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 USING REMOTE VIDEO IDENTIFICATION SYSTEM

CONTENTS

1 INTRODUCTION

"Certificate Policy and Practice for Providing a Registration Authority Qualified Service for Identification and Verification of Specific Attributes for Issuing a Certificate using a Remote Video Identification System" (the Policy/CP-CPS-RA-R/Certificate policy and practice for providing Registration authority qualified service for identification and verification of specific attributes for issuing a certificate using remote video identification system) is a document describing the general rules and norms applied by Evrotrust Technologies AD (Evrotrust) for providing a Registration Authority service whereby it verifies natural and legal persons' identity and, when necessary, specific attributes related to the persons, using a remote video identification system. The system of Evrotrust has been certified as ensuring a level of assurance equivalent to physical presence with regard to reliability. The equivalent level of assurance is confirmed by a Conformity Assessment Body pursuant to Art. 24, par. 1 (d) of Regulation (EU) No 910/2014. Evrotrust's remote video identification system has two varieties for providing the electronic identification service. Depending on the context of applicability of the electronic identification tool, the natural and legal persons who are identified and checked for specific attributes are remotely given the opportunity to use the Evrotrust mobile application or a web interface.

The service is provided for trust service providers (providers/TSPs) - clients of Evrotrust, and for Evrotrust's own needs. The natural and legal persons subject to remote identification and verification of specific attributes are users of such TSPs. The verification is performed in an automated way, and is confirmed by a Registration Authority (RA), which may be an internal structure of Evrotrust, or an external legal person to which Evrotrust has assigned the activity by virtue of contractual relations. As a result from the verification of identity performed by a Registration Authority of Evrotrust, the TSP provides an identification means, trust services and issues certificates for electronic signatures/seals.

Evrotrust, in its capacity as a qualified trust service provider, offers a system for electronic identification through a smart device or a computer to the users of the providers. The service allows for a quick, easy, reliable and secure creation of a user identification account, as well as secure authentication of users' data before third parties. Among the advantages of the provided service is an exceptionally quick and easy identification - anywhere, anytime. Using the completely digitalized electronic identification service is in full compliance with the legislation in force. Access

to the service is not geographically limited for all persons who have a valid identity document.

1.1 OVERVIEW

For the purposes of electronic identity authentication using a remote video identification system by an RA of Evrotrust, the procedures which are implemented provide high level of reliability and security of the verified information which identifies the TSP users. The procedures which are implemented ensure reliability and security during confirmation and revocation of the identification status of a particular person. The TSPs [Trust Service Providers] themselves implement analogous procedures which ensure reliability and security during the issuance of qualified certificates and the cryptographic keys related to them. The relations between Evrotrust that provides an RA service and the TSPs which are clients of the service are settled by virtue of a contract.

This document is a public one. It may be altered by Evrotrust at any time, each new revision being notified to the interested parties by publishing it in the Documents section on the Evrotrust website. https://www.evrotrust.com.

1.2 COMPLIANCE

Policy and practice for providing a qualified service to a Registering Authority for identification and verification of specific attributes for issuing a certificate through a remote video identification system 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 Protection Regulation);
- Law for the electronic document and electronic trust service (ZEDEUU);
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy

Requirements for Trust Service Providers;

- ETSI EN 319 411-1 General requirements;
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects;
- Art.13, para.1, letter "a" of the Directive (EU) 2018/843 of the European Parliament and of the council of 30 may 2018 amending directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending directives 2009/138/EC and 2013/36/EU;
- Atr. 42 from the Regulations for the Implementation of the Law on Measures Against Money Laundering;
- Atr. 55, para. 2 from the Law on Measures Against Money Laundering.

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.

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 using a Remote Video Identification System", with object identifier/OID: 1.3.6.1.4.1.47272.2.16.17.1.2.

1.4 POLICY MANAGEMENT

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

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. Contact person for the purposes of managing the document is 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

The terms used in this document are defined in Regulation (EU) No. 910/2014, including:

„Electronic identification" means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;

"Electronic identification scheme" means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;

"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;

"Web Interface" is a user interface developed by Evrotrust that provides individuals, legal entities or an individual representing a legal entity easy and fast registration and identification through the camera of their personal computer or mobile device;

"Authentication" means an electronic process that enables the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form;

"Relying Party" means a natural or legal entity that relies on the authentication service for electronic identification;

"**Electronic document**" means any content stored in electronic form, in particular text or sound, visual or audio-visual recording.

3 REGISTRATION AUTHORITY

The Registration Authority is an individual structure of Evrotrust, but it may also be an external legal person (subcontractor), to which the company assigns to carry out activities for the registration, identification and identity authentication of the users of a provider.

In order for a TSP to issue identification means and/or a certificate, the RA of Evrotrust, by appropriate means and complying to the national laws, shall verify the identity and, if applicable, all specific data for the natural/legal person to whom the provider is about to issue a certificate. The RA performs an authentication 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. Each operator registers with a unique number in the system of Evrotrust and a remote qualified electronic signature is issued to him/her and used by the operator for confirmation of successfully performed identification.

The RA operators have at their disposal a computer system, a tablet, a smartphone and/or other mobile devices which are necessary for the operators to carry out their activities. The hardware used by the operators meets the technical requirements for normal installation and functioning of an Evrotrust application and/or web interface, depending on the context of the service provided. The application has a mobile interface developed by Evrotrust, which can be installed both on the operator's device as well as on the device of the TSP user, allowing for the service to be used. Video calls held by the operators comply with internal procedures and a developed Evrotrust methodology. The RA operators enter the information collected while providing the identification service in the information system of the provider, in accordance with a form specified and approved by the management body of the TSP and templates for information collection.

Contact information of the RA of Evrotrust is available on the webpage of Evrotrust, at the following address: https://www.evrotrust.com.

4 OPERATING ACTIVITIES OF THE REGISTRATION AUTHORITY

The remote electronic video identification system has been certified as a system ensuring a level of security equivalent to physical presence by an independent certifying Conformity Verification Body pursuant to Art. 24, par. 1, d of Regulation (EU) 910/2014. Using the camera of his/her device or computer, the person takes a photo of a nationally admissible identity document. The system of Evrotrust performs an automatic recognition of the text in the MRZ zone and in the main text fields of the identity document, the protective elements of the document are analysed, and, when possible, the data from the identity document is compared to a reliable data source (reading the data through an NFC technology of the smart device, for example) or to a primary data source (for example, to the national database of identity documents, which, for Bulgaria, is the Ministry of Interior, or to a national register of the population). In these cases, the identity document validity is verified in an automated way, and the person's data is received. Upon successful verification, automated video identification is performed via specially developed technology for recognition of faces from the camera.

Remote identification by an RA operator is performed if the automated video identification is unsuccessful, or if, due to impossibility of integration with national primary databases or reliable sources of data of the citizen of the respective country, a photo of the person cannot be extracted through identity documents or by technological means. Upon unsuccessful identification (for example, if the data from the identity document cannot be read, if there are mistakes in the data, or due to any other reason), the identification process is redirected to an operator at the RA of Evrotrust for a video conference call.

During the identification process, the information by the TSP users is collected and verified. Evrotrust guarantees that the information contained in the certificates issued by the provider is true and correct at the time of their issuance. 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 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.

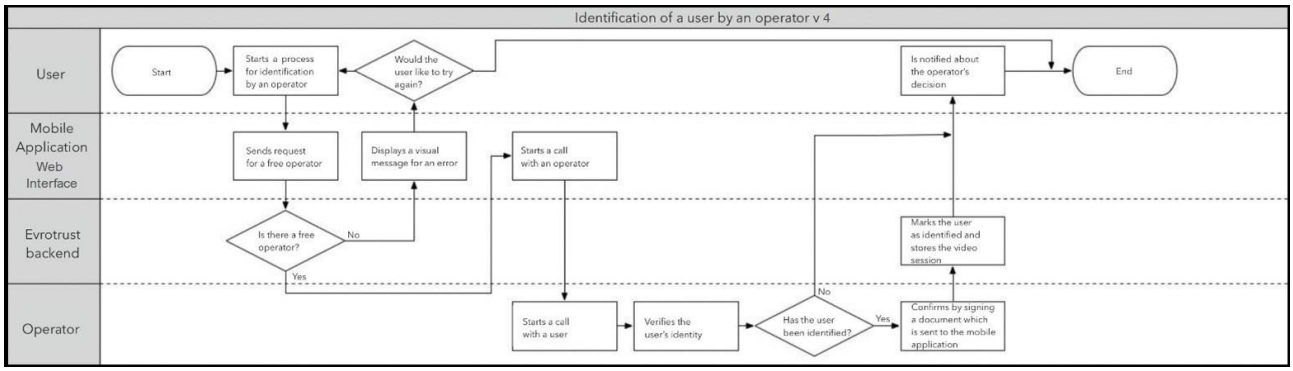
Personal data are processed in a way that guarantees high level of security, including protection against unauthorized or illegal processing, and against accidental loss, destruction or damage, by applying appropriate technical and organizational measures ("integrity and confidentiality").

The remote identification system has been verified by a Conformity Verification Body as a system ensuring a level of security equivalent to physical presence, pursuant to Art. 24 (1), item "d" of Regulation (EU) 910/2014.

4.1 REMOTE IDENTIFICATION OF A NATURAL PERSON

The remote video identification system of Evrotrust has been developed in a way that allows for the person's personal data to be entered in the system in an automated way, after scanning the identity document. In order for identification of the person to be performed, the TSP user should have installed a mobile application of Evrotrust on his/her smart device (such as a smartphone or a tablet), a mobile application with an integrated Software Development Kit (SDK) of Evrotrust or to have access to the web interface for providing the service using a standard web browser. Evrotrust initiates a procedure for verifying the validity of the identity document through a national database of identity documents (where the respective integration exists), or through reliable data sources. When possible, a photo of the person is received, with a resolution which allows automated processing. A procedure is implemented for an automated analysis of the person's biometrics through a series of control checks aimed at establishing that the identity of the person corresponds to the photo taken, including also 3D object verifications, in accordance with a certified methodology. The video recordings from the process of TSP users identification also go through a mandatory verification by an operator at the RA of Evrotrust. When verifications of the person have been successful, it is further preceded with issuing from the provider of an electronic means with authenticated personal data and/or a qualified certificate. In the case of approval, the operator confirms that identification has been successfully performed. If, while reviewing the video recording, the operator demonstrates any doubts with regard to details from the process, he/she rejects and suspends the person's identification, or he/she gets in touch with the person in order to clarify the procedure.

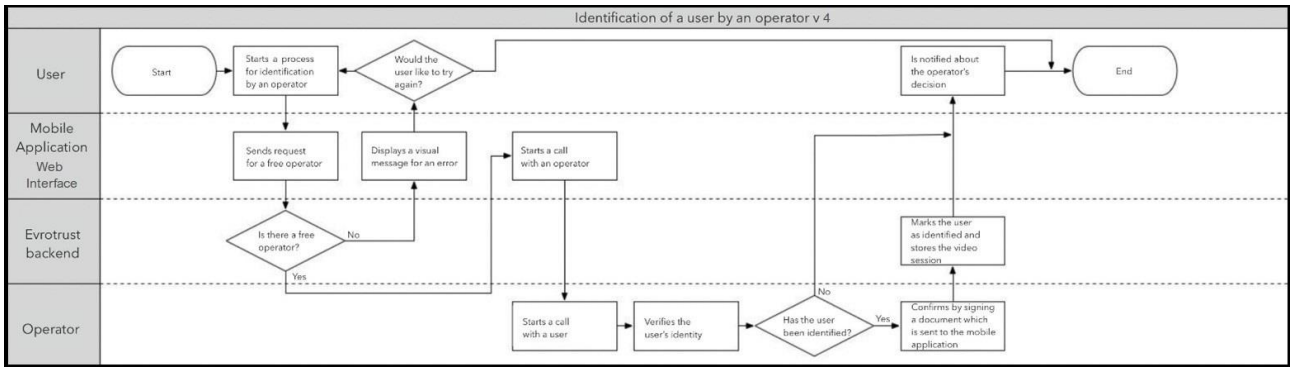
The process for automatic identification of a TSP user follows the scheme below:



When the person experiences difficulties during the automatic identification, he/she may initiate remote video identification with an operator at the RA of Evrotrust through his/her mobile device or via web interface, depending on the provided service. Verification of a natural person's identity is performed during a video conference call with an RA operator, by verifying an identity document. For the purposes of identification, the person must be a holder of a valid identity document. The person shows an identity document, a photo of which has been taken in advance, to a camera. A valid document shall be considered to be an identity card, an international passport, a diplomatic passport, a seafarer's passport, a foreigner's identity card, and other documents in accordance with the national legislation of the citizen of the respective country. In the case of an invalid document, the operator terminates the connection with the person, and the person should once again take a photo of the document and get in touch with the operator through the application. The operator compares the photo from the identity document to the person who is talking and asks control questions. Upon successful identification, an account of the person is automatically created in the system of the provider. A document for performed identification of the person is generated by a server, and a request for issuing a qualified certificate is sent to the certifying authority of the provider.

Upon unsuccessful identification, the person is invited to visit an office of the RA of Evrotrust.

The process of user identification by an RA operator follows the scheme below:



The minimum set of natural person's personal data which is collected and verified for the purposes of identification depends on the context of provision of the service – via mobile application or a web interface, and is specified below:

a) family name (or names) – in both cases;

b) given name (or names) – in both cases;

c) date of birth – in both cases;

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. (in the Republic of Bulgaria - a Personal number [EGN]/Personal number of a foreigner) – in both cases;

e) number of personal identification document – in case of identification via web interface.

The set of natural person's data may have additional specific data 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) phone number;

f) e-mail address;

g) date of issue of personal ID document;

h) date of expiration of personal ID document;

i) 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 data).

Evrotrust verifies the information authenticity using all legally permitted means in the respective primary registers.

4.2 REMOTE IDENTIFICATION OF A NATURAL PERSON 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.), where representative power is granted by operation of law, remote verification of the legal person is performed in the official registers (in Bulgaria, for example, it is performed in the registers kept by the Registry Agency). The verification is performed on the basis of a unique national identifier entered in the application of Evrotrust 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). For the natural person, identity verification is performed pursuant to item 4.1 in a national register or in a reliable source.

The mobile application/SDK of Evrotrust has been developed in a way that allows a natural person, who is a representative of a legal person, to activate a functionality of the application for performing identification. In order to do this, the person should have installed a mobile application of Evrotrust on a smart device (such as a smartphone or a tablet), or a mobile application with an integrated mobile SDK of Evrotrust.

In case of remote identification through a web interface, it is necessary for the person to open a website in a pre-known and supported browser, in which the solution of Evrotrust for remote electronic identification through a web interface is integrated.

In case that the automated verification is unsuccessful, it is further proceeded with a video identification with an RA operator. In the case of approval, the operator confirms that identification has been successfully performed by signing the session electronically, through the mobile application of Evrotrust. If, while reviewing the video recording, the operator demonstrates any doubts with regard to details from the process, he/she rejects and suspends the person's identification, or he/she gets in touch with the person in order to clarify the procedure.

The legal person's identity verification aims at proving that, during consideration of the request for issuing a qualified certificate, the legal person is existing and that the representing person that applies for a qualified certificate has representative powers to request the issuance.

During verification, the operator may suspend the process of identification for the purposes 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;

b) in case that 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 rendered commercially insolvent;

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

Evrotrust takes measures to minimize the risk of the legal person's identity not corresponding to the declared one. Evrotrust verifies the information authenticity by all legally permitted means in the respective public registers and reliable sources.

5 USE AND APPLICABILITY OF A REGISTRATION AUTHORITY SERVICE FOR ELECTRONIC IDENTIFICATION BY A REMOTE VIDEO IDENTIFICATION SYSTEM

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 electronic identification and qualified certificate management in accordance with the applicable laws and the good practices regarding data protection and retention. Data is stored for a period consistent with the requirements of the internal and independent audits which are performed, as well as for

the purposes of security breach investigations. Unless otherwise required, after using it for its intended purposes, the collected data is destroyed in a secure way.

7 PHYSICAL SECURITY CONTROL

The measures which are taken for physically protecting Evrotrust are an element of the Information Security System developed and implemented in Evrotrust and complying with 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 the undermining of resources;
- undermining or stealing information or information processing means.

7.1 THE PHYSICAL ACCESS

The offices of the RA of Evrotrust are individual premises, 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) and authorized employees of clients.

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 the employees 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 misled 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 FREQUENCY OF TRAININGS 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 an 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 breakdowns in services or technologies. In order for all this to happen, Evrotrust constantly monitors all systems and services (24x7x365).

The Plan indicates the approximate time for detecting any types 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 Incident Management 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 Business Continuity Plan for the cases when accidents occur, such as major system or network 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 performed in Evrotrust 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, 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 AUDIT BY THE NATIONAL SUPERVISORY BODY

The National Supervisory Body may, at any time, carry out an audit, or request that a Conformity Assessment Body perform an 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 (TSPs) 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 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 by the RA operators of the requirements for confidentiality and non-distribution of personal data of persons that became known during the performance of the identification activity.

17 LIABILITIES, RESPONSIBILITY AND GUARANTEES OF THE REGISTRATION AUTHORITY

Evrotrust guarantees that the RA fulfils 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.