CERTIFICATE POLICY AND PRACTICE

FOR PROVIDING AN ELECTRONIC IDENTIFICATION SERVICE

Version: 1.0

CONTENTS

1. INTRODUCTION

Evrotrust Technologies AD (Evrotrust) is a legal entity, entered in the Commercial Register to the Registry Agency with UIC 203397356, having seat and management address at: the city of Sofia, Izgrev District, residential complex Iztok, 2, Nikolay Haytov St, entr. 5 /Д/, fl. 2, contact phone number: +359 2 448 58 58, Internet address: http://www.evrotrust.com. The company performs public functions pursuant to the Electronic Document and Electronic Trust Services Act (EDETS) and provides public services pursuant to the E-Governance Act.

Evrotrust is a qualified trust service provider. It provides users with qualified trust services and products with high level of security in the territory of the Republic of Bulgaria, as well as in EU member-states and other countries around the world.

Evrotrust offers its clients (a relying party) a trust service of electronic identification through a smart device, the service being based on qualified trust services for which the provider is entered in the Trusted List of qualified trust service providers. The service allows for a quick, easy, reliable and secure user account creation, offering users a possibility for secure authentication of their data before relying parties. Among the advantages of the provided service is a quick and easy identification - anywhere, anytime. Using a service of electronic identification is in full compliance with the legislation which is in force and is based on the use of qualified electronic signatures. Access to the service is not geographically limited for all persons who have a valid identity document.

The service satisfies the needs for identification through a trusted service pursuant to Art. 13, par. 1, item "a" of 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, and pursuant to Art. 42 of the Regulations on applying the Measures against Money Laundering Act, in conjunction with Art. 55(2) of the Measures against Money Laundering Act.

1.1. OVERVIEW

"Certificate Policy and Practice for Providing a Electronic Identification Service" (“the Policy”/CP-CPS-IdV/Certificate policy and practice for providing a identification service) is a document describing the general rules and standards applied by Evrotrust Technologies AD (Evrotrust) for verification of personal data of natural and legal persons or, where necessary, of any specific attributes related to such persons, and for issuance of qualified and other certificates which contain such data. This document describes the general requirements for provision of the electronic identification service, as well as the security measures, rights and obligations for all participants in the infrastructure of the public key of Evrotrust, including certifying authorities, corporate clients, end users and relying parties. The service allows for a secure and

reliable creation of a statement for provision of personal or other data, issuance of a qualified attribute certificate for a qualified electronic signature whereby the statement with personal or other data is signed, remote signing of the statement with a qualified electronic signature accompanied by the attribute qualified certificate, as well as providing third parties with the signed statement.

This document forms an inseparable part of the General Terms and Conditions of the Contract for Provided Trust, Information, Cryptographic and Consulting Services. This document has been drawn up in full compliance with Regulation (EU) No 910/2014, Regulation (EU) 2016/679 (GDPR), as well as with the legislation applicable in the Republic of Bulgaria. The Policy is a public document and cannot be amended by Evrotrust at any time. Interested parties shall be informed of each new revision, which shall be published on the website of Evrotrust. https://www.evrotrust.com/landing/bg/a/tsp-documents.

1.2. COMPLIANCE

Evrotrust provides a service of electronic identification, covering the requirements of item 5.5.1.3 (g) 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/IdV.

This document 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);
- 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.
- Art. 13, par. 1, item "a" of 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.
- Art. 42 of the Regulation on applying the Measures against Money Laundering Act;
- Art. 55, par. 1 of the Measures against Money Laundering Act;

The activities of Evrotrust related to the provision of the electronic identification service have already been verified by an independent verification organisation 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: “Certificate Policy and Practice for Providing a Electronic Identification Service”, with object identifier (OID): 1.3.6.1.4.1.47272.2.16.17.3.

1.4. PARTICIPANTS IN THE INFRASTRUCTURE

1.4.1. CERTIFYING AUTHORITY *EVROTRUST RSA OPERATIONAL CA*

Evrotrust RSA Operational CA performs the following specific obligations:

- Accepting an electronic request for issuing qualified attribute certificates;
- Issuing a qualified attribute certificate;
- Publishing and maintaining issued qualified attribute certificates in accordance with the procedures described in the "Policies and Practices" of Evrotrust;
- Remote signing with a qualified electronic signature;
- Keeping the records (logs) for the electronic identification process, issuing qualified attribute certificates, and remote signing with a qualified electronic signature.

All qualified user certificates which the Operating Certifying Authority issues are described in the document "Certification Practice Statement for Providing Qualified Trust Services"

1.4.2. USERS

Any natural or legal person which has a contract with Evrotrust for a electronic identification service is a user of this service.

When this is practically possible, the provided trust service is accessible also to disabled people.

1.4.3. RELYING PARTIES

For the purposes of its activity of providing an electronic identification service, relying parties shall be such corporate clients as banks, insurance companies, state organisations, telecom operators, etc., which have concluded an integration contract with Evrotrust, and which rely on the trust service for the

purposes of establishing business relations, professional, administrative, or other relations, or for the purposes of carrying out various operations or transactions. These may be banks, insurance companies, state organisations, telecom operators, etc. Relying parties should have knowledge and skills concerning the use of qualified attribute certificates and they should rely on the circumstances certified by them only with regard to the applicable Policy, especially when it concerns the level of security while verifying the identity of the persons to whom the qualified attribute certificates have been issued, or when it concerns limitations on certificate use listed in the certificates. Relying parties have constant access to the Evrotrust registers in order to verify the validity of the qualified attribute certificates. Relying parties established outside the territory of the Republic of Bulgaria can count on a reliable, secure, easy and convenient automated qualified validation of qualified electronic signatures for which the attribute certificates are issued.

1.4.4. OTHER PARTICIPANTS

Evrotrust reserves the right, whenever necessary, to enter into contracts with external parties for the provision of services related to the trusted service of electronic identification.

1.5. APPLICABILITY AND USE OF ELECTRONIC IDENTIFICATION

1.5.1. APPLICABILITY OF THE SERVICE

The applicability of the electronic identification service is related to Evrotrust authenticating personal and other data of natural and legal persons, such data being included in the issued qualified attribute certificates, as well as in users' statements for the provision of personal and other data upon request of a relying party. Evrotrust takes appropriate technical and organizational measures during provision of the service, in order to avoid any possible data security breaches. Personal and other data are processed in a way that guarantees their 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.

1.5.2. USE OF THE ELECTRONIC IDENTIFICATION SERVICE

Users can make a one-time use of the data verified in the qualified attribute certificates to sign a statement for personal data; in this way, they identify themselves and agree to the provision of data. Once registered, such persons may use their registration and make electronic identification without limitation to the number of times; however, each validation shall require the use of a newly generated one-time private key with a new qualified attribute certificate. The validity period of the qualified attribute certificate and its

related private key is 2 (two) hours.

1.5.3. USE OF A QUALIFIED ATTRIBUTE CERTIFICATE BY RELYING PARTIES

Relying parties shall use the person's data authenticated in the attribute certificates and declared by the users only after verifying the status of such data and the electronic signature of the certifying authority that has issued the certificate.

Evrotrust does not bear responsibility if the relying party does not make such verifications, if it is not entitled to process the user's personal data, or if it processes them in breach of the applicable legislation.

1.5.4. PROHIBITION ON THE USE OF THE ELECTRONIC IDENTIFICATION SERVICE

The electronic identification service shall not be used in a way which may lead to a breach of data confidentiality, integrity and security.

1.6. MANAGEMENT OF THE POLICY AND OF THE PRACTICE

The Management Body of Evrotrust is responsible for managing this document.

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. Users are obliged to follow only that version of the Policy which is valid as at the time of using the service.

Contact person for the purposes of managing the document “Certificate Policy and Practice for Providing a Electronic Identification Service" is the CEO of Evrotrust.

Additional information may be received at the following address:

Evrotrust Technologies AD

Sofia, 101, Tsargiradsko Shosse Blvd,

ACTIVE Business Center, fl. 6

Phone number: + 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:*

"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;

"Authentication" means an electronic process that enables the electronic identification of a natural or legal person or the origin and integrity of data in electronic format to be confirmed;

"Relying party" means a natural or legal person that relies upon the trust service of electronic identification;

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

3. PUBLIC REGISTER

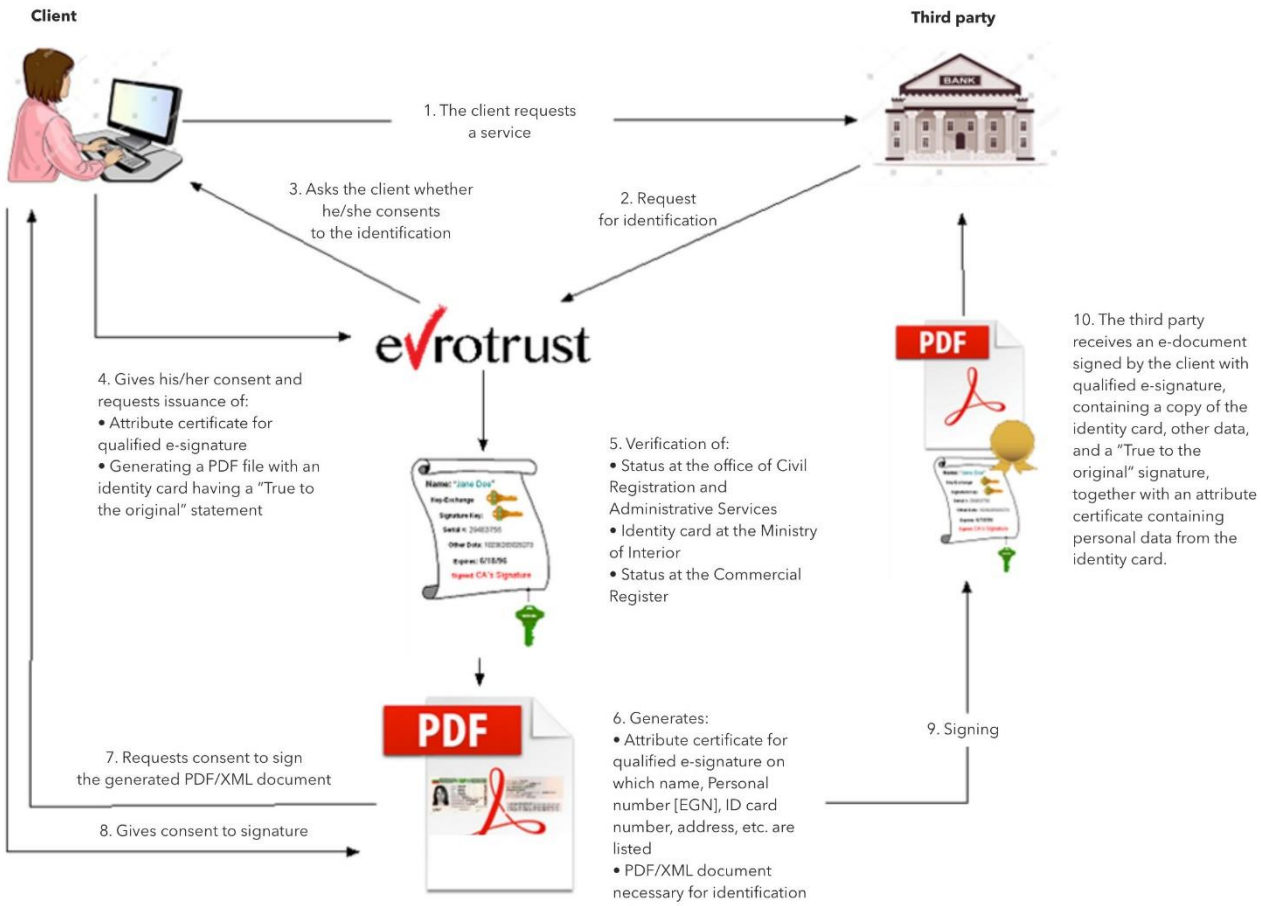
The Public Register of Evrotrust is a repository holding current and previous versions of electronic documents (Policies and Practices, certificates of certifying authorities, and other types of information) to be used by users and interested parties. The repository is managed and controlled by Evrotrust. Access to the information is provided constantly (24/7/365). The Public Register is accessible through the webpage of Evrotrust: https://www.evrotrust.com, the access being provided via HTTP/HTTPS protocol. Evrotrust has taken measures, logical and physical mechanisms for protection against unauthorized addition, removal, or change in the information published in the repository. In case any violations are found out, Evrotrust shall take appropriate actions to retrieve the entire amount of information. If necessary, Evrotrust shall impose legal sanctions, notify the entities concerned, and compensate them for their losses.

4. OPERATING ACTIVITIES FOR PROVIDING AN ELECTRONIC IDENTIFICATION SERVICE

Evrotrust verifies the identity of a person by using a system for remote identification of natural/legal persons. The operating activities for providing an electronic identification service include issuing an attribute certificate for electronic signature and generating a statement for personal and other data provision signed with the issued certificate and served to a relying party upon the request of an Evrotrust user. Evrotrust guarantees that the information contained in the attribute certificates is true and correct as

at the time of their issuance. The request for a remote use of a trust service of electronic identification is received upon request of an Evrotrust user for the purposes of establishing, altering, or terminating their legal relations with the relying party which is a client of the Evrotrust service (such as a bank, an insurance company, etc.) via a specially developed communication interface.

4.1. SCHEME OF THE ELECTRONIC IDENTITY AUTHENTICATION PROCESS



For the purposes of identity authentication, the natural person, in his/her personal capacity, or as a representative of a legal person, assigns Evrotrust to: issue an attribute qualified certificate for electronic signature, create a document - statement for electronic provision of personal and other data, remotely sign with a qualified electronic signature accompanied by the attribute certificate and provide the signed statement with the attribute qualified electronic signature to a relying party.

The service provision process is initiated by a relying party which sends Evrotrust a request asking the user for identification through a specialized web portal, API interface, or through an SDK module. The user assigns Evrotrust to generate for him/her the statement with the requested . The statement for

personal data provision is made available to the person in a readable PDF format through the mobile application or through the signature portal of Evrotrust, so that the person can review the statement before signing it. An XML file is also added to the statement, containing the same data in a machine-readable format, for automated processing by the relying party. In the event that the person is not an Evrotrust user, they must go through a registration and identification process with Evrotrust and become an Evrotrust user. The data which the relying party may request from the Evrotrust user may consist of (non-exhaustively):

- for a natural person - family name (or names), given name (or names), date of birth, 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), mobile phone number and e-mail address. Additional specific data which might be collected by the operator/the agent are: given name (or names) and family name (or names) at birth, place of birth, permanent address and sex. Evrotrust reserves the right, depending on the implementation of the integration with the different types of identity documents, with primary registers and reliable data sources, to add to the set of specific data;
- for a legal person and for the natural person representing it (managers, board members, authorized agents, etc.), where representative power is granted by operation of law, remote verification and collection of the legal person data are performed in the official public registers (in Bulgaria, for example, a verification is performed in the registers kept with the Registry Agency). The verification is performed on the basis of a unique national identifier entered in the Evrotrust application 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, an identity verification is performed pursuant to the paragraph above.

The methods for persons' identification are developed and described in the documents of Evrotrust: "Policy and Practice for providing a service of a registration authority for Identification and verification of specific attributes for Issuing a certificate by means of physical presence" and "Policy and Practice for providing a service of a registration authority for identification and verification of specific attributes for issuing a certificate via a remote video identification system".

Evrotrust verifies the information authenticity using all legally permitted means. The validity of an identity document of a natural person is verified through the national identity documents database (in case the respective integration is available), through reliable data sources, by personal presence, or by operator's identification. For establishing the identity of a legal person, as well as its representatives (managers, board members, authorized agents, etc.), when representative power is granted by operation of law, a verification of the legal person is performed in the official register, based on a unique national

number which shall remain unchanged for as long as possible (in the Republic of Bulgaria, for example, such is the UIC [Unified Identification Code]/BULSTAT).

For verification of the identity of natural and legal persons, and, if necessary - of specific attributes related to the persons, Evrotrust uses a remote video identification system. The remote identification system has been verified and certified 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.

When a relying party submits a request for identification by a specific Evrotrust user, Evrotrust sends a message to the user's smart device in the mobile application, whereby it asks for the user's consent to the identification. The person is provided with an opportunity to familiarise themselves with the scope of personal and other data that are required by the relying party, so that they can make a decision whether to make an identification or not.

Following the activation of a functionality whereby the user states his/her wish to identify himself/herself, and upon the user's assignment, Evrotrust draws up a document - statement for personal data provision, generates a pair of cryptographic keys, and issues an attribute qualified certificate for the public key from that pair, providing an opportunity for the person to sign the statement for provision of personal and other data. The user enters their PIN/biometrics, thus remotely activating the private key kept on the Evrotrust HSM in a protected room, which leads to the creation of a qualified electronic signature on the statement for provision of personal and other data, on the basis of the attribute certificate. The attribute certificate issued by Evrotrust is a one-time certificate, has short validity period, and contains a verified public key, identity document data and additional attributes beyond the mandatory ones for a qualified certificate resulting from Regulation (EU) No 910/2014, in accordance with the applicability of the certificates and the client's contractual relations. 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.

The qualified attribute certificates issued by the Certifying Authority of Evrotrust - Evrotrust RSA Operational CA - meet the requirements of Regulation (EU) 910/2014 and are acknowledged in the European Union. Taking into account the cross-border interoperability of the formats of the qualified electronic signatures introduced by Regulation (EU) No 910/2014, the qualified attribute certificates do not exceed the mandatory requirements set out in Regulation (EU) No 910/2014 and Regulation (EU) 2015/1501[1] regarding the requirements for the minimum set of person identification data uniquely representing any natural or legal person.

[1] *COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*

The process of attribute certificate provision is described in the document "Certificate Policy and Practice for providing a service of issuing an attribute certificate".

The relying party receives, via an interface agreed upon with Evrotrust, the signed PDF/XML file with the user's statement for provision of personal and other data, signed with the attribute qualified certificate.

4.2. TERMINATING THE CONTRACT WITH EVROTRUST

A contract for providing an electronic identification service which is accessible via the Evrotrust application shall be terminated upon cancelling an user account.

4.3. IDENTIFICATION AND VERIFICATION OF IDENTITY AFTER CANCELLING AN ACCOUNT

Where a functionality is activated through the mobile application of Evrotrust for deleting an account, and where in time a person wishes to have an identification service provided, such person must pass through a new process of registration and identification.

5. PHYSICAL SECURITY CONTROL

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 described in the document named "*Certification Practice for Providing Qualified Trust Services*".

5.1. PREMISES AND PREMISES STRUCTURE

Evrotrust has a specially designed and equipped room, with the highest degree of physical access control, which houses Certifying Authority of Evrotrust as well as all central components of the infrastructure.

5.2. PHYSICAL ACCESS

The physical security of the systems for issuing and managing certificates, and for creating and managing electronic identification complies with the requirements of international standards and recommendations.

Physical integrity is ensured for the equipment in the secured and isolated room of Evrotrust. There are two-factor access control and 24-hour physical security. Physical access to the critical equipment is not allowed for more than 30 (thirty) minutes per visit. Access to the equipment cabinet is not allowed with less than 2 (two) authorized Evrotrust technicians. Each access to the critical infrastructure premises is documented in special journals.

Protection of the Evrotrust building is realized by 24-hour security. On the Evrotrust premises, there are an alarm system, a video surveillance system, a signal-alarm system, and an access control system.

The physical security of the systems is described in the document "Certification Practice for Providing Qualified Trust Services".

5.3. STORAGE OF DATA CARRIERS

All carriers containing software, data archives or audit information are stored in a strongbox, in rooms with special access and implemented access control. In the room with the archive of Evrotrust, there is a system of physical and logical protection. Recording and storage of significant information is performed by means of an effective record management system, taking into account the applicable legislation and the good practices with regard to data protection and storage. Evrotrust keeps a database where it stores information about the activities concerning the provision of electronic identification. The database is kept on a differential basis: Database, File Systems and Archives.

5.4. WASTE DISPOSAL

Electronic carriers containing significant security information of Evrotrust are destroyed after expiration of the storage period specified in accordance with the internal rules. The carriers of information about cryptographic keys and access codes used for their storage are shredded in the appropriate devices. This applies to carriers which do not allow for stored data to be permanently destroyed or reused. In specific cases, the information from portable carriers is destroyed through deletion or formatting of the device, without any option for recovery.

6. ORGANIZATIONAL CONTROL

All security procedures for issuing, administering and using qualified attribute certificates, and for creating and managing electronic identification, are performed by trusted staff of Evrotrust. Evrotrust keeps sufficient number of qualified employees so that, at any time during the performance of its activities, such employees can ensure compliance with the legislation which is in force and with the internal rules and regulations of the company.

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

7. EVENT RECORDINGS AND MAINTENANCE OF JOURNALS

In order to ensure effective management and functioning of Evrotrust, all events that have significant importance to the security and reliability of the technological system, to staff and user control, and the impact on the security of the provided services, are recorded. Evrotrust guarantees a high level of personal data security during such data processing and encryption. In case of an incident, the stored records can be quickly recovered.

Information about the electronic journals is generated automatically.

Journals with records of registered events are stored in files on the system disk for at least 6 (six) months. During this time, they are available online, or in the process of searching by authorized employees of Evrotrust. Following this period, the records are stored in the archives. Archived journals are kept for at least 10 (ten) years, after that they are destroyed in a secure way.

The archive is signed by an electronic signature/an electronic time stamp. The information from the log records is periodically recorded on physical carriers, which are stored in a special safe, located in a room with high level of physical protection and access control.

8. VULNERABILITY AND ASSESSMENT

Evrotrust classifies and maintains registers of all assets in accordance with the requirements of ISO/IEC 27001. In accordance with the "Security Policy" of Evrotrust, an analysis is carried out of the vulnerability assessment for all internal procedures, applications and information systems. Analytical requirements may also be determined by an external institution authorized to perform an audit of Evrotrust. Risk analysis is performed at least once a year. The decision to initiate an analysis shall be taken by the Board of Directors.

9. ARCHIVING

Evrotrust archives all data and files related to: information for the registration; to system security; to all requests sent by users; all the information about the users; all keys used by the Certifying Authorities and by the Registration Authority; as well as to all the correspondence between Evrotrust and the users. Subject to archiving are all documents and data used throughout the process of identity verification.

10. TERMINATING THE ACTIVITIES OF EVROTRUST

The obligations described below have been developed in order to ensure minimal interruptions in those activities of the users and of the relying parties which result from the Evrotrust decision to terminate its operations.

10.1. TERMINATING THE ACTIVITY OF A CERTIFYING AUTHORITY

Upon terminating the activity of a certifying authority, Evrotrust takes the following actions:

- It follows a plan and scenario which is updated and approved by the Management for terminating the activity of a certifying authority;
- It informs the users, the Supervisory Authority, and the third parties that the activity of its certifying authority has been terminated. The information shall be provided by email, or by publication on the website of Evrotrust.
- It terminates the authorization of all persons having contractual obligations to perform activities related to that particular certifying authority;
- Before the activity of the certifying authority is terminated, within a reasonable timeframe, it transfers its obligations related to maintenance of all the information necessary for providing evidence, to a reliable party;
- Before termination of the activity, the private keys, including their duplicate copies, are destroyed or withdrawn in such a way that personal keys cannot be extracted;
- If possible, it transfers its activity to another qualified provider;
- Evrotrust takes measures to cover the costs in case of bankruptcy, or any other reasons due to which the activity of a certifying authority is terminated. In case Evrotrust is unable to cover such costs on its own, it has provided for measures to be taken within the applicable legislation;
- It changes the status of the operating certificate;
- It suspends the issuance of new certificates, but continues to manage active certificates until their expiration;
- It makes reasonable commercial efforts to minimize violation of users' interests.

Evrotrust supervises and does not permit the issuance of a certificate for a period longer than the validity period of the issuing certifying authority.

10.2. TRANSFER OF ACTIVITY TO ANOTHER QUALIFIED TRUST SERVICE PROVIDER

In order to ensure uninterruptedness of the issuance of qualified trust services for users, Evrotrust may sign an agreement with another qualified trust service provider. In such case, Evrotrust:

- notifies the Supervisory Authority for its intention not later than 2 months before the date of termination and transfer of activity;
- makes any effort and care to continue the validity of the issued user certificates;
- notifies the Supervisory Authority and the users, in a written form, that its activity is taken by another qualified provider, specifying its name. Such notification is published on the webpage of Evrotrust;
- notifies the users about the conditions for maintenance of the information transferred to the receiving provider;
- changes the status of the operating certificates and duly transmits all the documentation related to its activity to the receiving provider, together with all archives and all issued certificates;
- performs all the necessary activities for transferring the obligations for information maintenance to the receiving provider;

The receiving provider takes over the rights, obligations and the archive of Evrotrust.

10.3. WITHDRAWAL OF THE QUALIFIED STATUS OF EVROTRUST

Upon revocation of the qualified status of Evrotrust, it shall carry out the following:

- inform the users about its changed status;
- change the status of its certificates;
- terminate issuance of new qualified attribute certificates;
- make reasonable commercial efforts to minimize violation of users' interests.

11. MANAGEMENT AND CONTROL OF TECHNICAL SECURITY

The procedures for generation and management of cryptographic keys and the related technical requirements are described in the document "Certification Practice for Providing Qualified Trust Services".

12. COMPUTER SYSTEMS SECURITY

Evrotrust uses only reliable and secure hardware and software that are part of its computer system. The computer systems on which all critical components of the Evrotrust infrastructure operate are equipped and configured with means of local protection for access to the software and the information data. Evrotrust uses information security management procedures for the entire infrastructure in accordance with standards generally accepted in the international practice.

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

12.1. TECHNOLOGY SYSTEM LIFECYCLE SECURITY

All hardware changes are monitored and registered by authorized Evrotrust employees. When a new technical equipment is purchased, it is supplied with the necessary operating procedures and instructions for use. Supervision of the technological system functionality is implemented and it is ensured that it functions properly, in accordance with the supplied manufacturing configuration.

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

12.1. NETWORK SECURITY

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

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

13. VERIFICATION AND CONTROL OVER THE ACTIVITY OF EVROTRUST

13.1. INTERNAL AUDITS

The purpose of the internal audits of Evrotrust is to control the provision of trust services and electronic identification, inasmuch as this activity is compatible with the integrated management system which is implemented and which includes the requirements of the ISO/IEC 27001[2], ISO 9001[3], ISO 22301[4], and ISO/IEC 20000-1[5] standards, and of Regulation (EU) No 910/2014, Regulation (EU) 2016/679[6], as well as the internal management decisions and measures. Evrotrust is 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.

13.2. INDEPENDENT EXTERNAL AUDIT

[2] *ISO 27001 Information technology. Security techniques. Information security management systems*
[3] *ISO 9001 Quality management systems*
[4] *ISO 22301 Societal security. Business continuity management systems*
[5] *ISO 20000-1 IT service management system*

Evrotrust is subject of audit at least once every 24 months by a Conformity Assessment Body. The purpose of the audit is to confirm that the trust services and electronic identification provided by Evrotrust meet the requirements set out in Regulation (EU) No 910/2014.

Evrotrust is subject to 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 activity of Evrotrust is 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 the Conformity Assessment Body perform an assessment of the conformity of Evrotrust's activity with the requirements of Regulation (EU) No 910/2014.

14. FINANCIAL RESPONSIBILITIES

Evrotrust is liable for the provided identity verification service to those persons who rely on identification. Evrotrust shall be liable if damages are caused due to its fault. If Evrotrust acknowledges and accepts that damages have occurred, it undertakes to pay such damages which are a direct and immediate consequence of the employees' negligence.

15. INSURANCE OF ACTIVITY

Evrotrust takes out a compulsory insurance of its activity, which shall also include its activities on providing the identification service. Evrotrust is liable for intentional damages, or damages that have occurred due to the negligence of a natural or a legal person because of its employee’s failure to fulfil their obligations.

16. INVIOLABILITY OF PERSONAL DATA

Evrotrust is registered as Personal Data Administrator pursuant to the Personal Data Protection Act. In its capacity as Personal Data Administrator, Evrotrust strictly observes the meeting by its employees of the requirements for confidentiality and non-distribution of personal data of persons that became known while carrying out activities for electronic identification.

16.1. INTELLECTUAL PROPERTY RIGHTS

The variety of data included in the qualified attribute certificates issued by Evrotrust are subject to intellectual property rights, or other material and non-material rights.

17. LIABILITIES, RESPONSIBILITY AND GUARANTEES OF EVROTRUST

17.1. GUARANTEES AND LIABILITIES

Evrotrust guarantees that it carries out its activity by:

- strictly complying to the conditions of this document, the requirements of Regulation (EU) No 910/2014, Regulation (EU) 2016/679, and the national legislation in the performance of its activity as a Qualified Trust Service Provider;
- ensuring that the provided service does not infringe copyrights and licensed rights of third parties;
- using technical equipment and technologies which ensure reliability of the systems and of the technical and cryptographic security during process implementation, including also a safe and secure mechanism/device for generating keys and creating an electronic signature in its infrastructure;
- issuing qualified attribute certificates for electronic signatures after verifying, by legally permitted means, the information which is provided;
- securely storing and maintaining information related to the attribute certificates which are issued and the operational work of the systems;
- complying with the established operating procedures and rules for technical and physical control, in accordance with the terms of this document;
- issuing certificates, upon request, in compliance with the terms and procedures of this document, the relevant internal procedures and generally accepted standards;
- notifying users of the availability of its qualified status;
- providing an opportunity for immediate termination of a qualified attribute certificate validity;
- immediately notifying the interested parties after a certificate has been terminated;
- ensuring that there are conditions for precise verification of the time of issuance and termination of the certificates;
- performing procedures for identification and verification of authenticity/identity of natural/legal persons;
- ensuring measures against forgery of attribute certificates and confidentiality of the data to which it has access during the process of creating the signature;
- using reliable systems for storing and managing the certificates;
- taking immediate measures in case of occurrence of technical issues related to security;

- upon expiration of the validity of the certificate, revoking its validity;
- informing users and relying parties on their obligations and due diligence while using or relying on the trust services provided by Evrotrust, and on the proper and safe use of the issued attribute certificates and the provided electronic identification related to them;
- using and storing the collected personal and other type of information solely for the purposes of its activity for providing electronic identification in accordance with the national legislation;
- not storing and not copying data for creating user's private keys;
- keeping available such means as to make its activity possible;
- concluding an insurance for the time of its activity;
- keeping trusted staff with the necessary expert knowledge, experience and qualification for carrying out the activity;
- maintaining Public Register/Repository;
- providing constant access to the Public Register electronically (24/7/365);
- ensuring protection against changes added to the Public Register kept by it, by means of unauthorized and unlawful access, or due to unforeseeable circumstances;
- providing conditions for each relying party to verify the status of an issued and published attribute certificate in the Public Register of certificates;
- performing periodic internal and external audits of its activity;
- using certified software and hardware as well as secure and reliable technological systems for its activity;
- maintaining, on the website of Evrotrust, a list of registration authorities, a list of recommended software and hardware for users, forms, templates, a standard contract, and other documents for the benefit of users;

17.2. RESPONSIBILITIES

Evrotrust bears responsibility to users and relying parties for damages caused by gross negligence or intent:

- from failure to comply with the requirements of Regulation (EU) No 910/201 in carrying out its activity of providing qualified trust services;
- from untrue or missing data in the qualified attribute certificate as at the time of its issuance;
- from the algorithmic incompatibility between the private key and the public key entered in the certificate;
- from failure to comply with its obligations to issue and manage qualified attribute certificates;
- from entering untrue or missing data in the certificates;
- from omissions in establishing the person's identity.

18. OBLIGATIONS OF USERS

The users of the identity verification service which is related to the issuance of qualified attribute certificates have the following obligations:

- to familiarize themselves and to comply with the terms and conditions of the Contract, of the Policies and Practices for electronic identification provision by Evrotrust, as well as with the requirements of other documents published in the Evrotrust Public Register;
- to provide true, correct and complete information, as required by Evrotrust in accordance with the Contract, legal requirements, and applicable Policies and Practices;
- in case of any discrepancy between the provided information and the verified content, the user must immediately inform Evrotrust;
- to confirm the terms and conditions set out in the Contract between the user and Evrotrust;

19. RESPONSIBILITY OF THE USER

The user's responsibility arises from the fulfilment of their obligations. The terms of responsibility are set out in a Contract with Evrotrust. The user shall be responsible to Evrotrust and to the relying parties in case that:

- the user does not comply with the exact requirements of this document;
- the user has made untrue statements which are related to the provided service;
- in case that a natural person without representative powers initiates an identification service for a legal person, such person shall be responsible for the damages.

20. DISCLAIMER

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

- illegal actions taken by users and relying parties;
- accidental events characterised as force majeure, including malicious acts of third parties (hackers' attacks, defrauding a mobile device, access to the identification method, etc.)
- request for an identity verification service submitted by a person who does not meet the requirements and does not follow the procedures of the "Policies and Practices" of Evrotrust.

21. DISPUTE RESOLUTION

Only dissimilarities or contradictions between persons who are parties to the contract with Evrotrust

may be subject to disputes. Disputes or complaints regarding the use of electronic identification and qualified attribute certificates provided by Evrotrust will be solved by intermediation, on the basis of information submitted in a written form. Claims shall be submitted in a written form, to the address of Evrotrust.

22. APPLICABLE LAWS

The provisions of the Bulgarian legislation shall apply to all issues which are not settled in this document.