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

CERTIFICATE POLICY AND PRACTICEFOR

PROVIDING A QUALIFIED ELECTRONIC IDENTIFICATION SERVICE

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 mobile/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. Electronic identification is a process using data in electronic format to identify persons whose data represent in a unique manner a given natural person or legal entity, or a natural person representing a legal entity. Electronic identification provides citizens with the possibility to access cross-border online services, their legal security and possibility for quick and easy interaction among business, public bodies and citizens. 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 qualified service of electronic identification is in full compliance with the legislation in force and is based on the use of qualified or advanced electronic signatures. Access to the service is not geographically limited for all persons possessing 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.

In order to provide electronic services, Evrotrust has at its disposal a legally recognized

means for secure remote certification and verification of the identity of citizens, certified in accordance with Regulation (EU) No. 2015/1502 for "high" level of assurance. The assurance level relates to an electronic identification means within the context of the electronic identification scheme of Evrotrust. The "high" assurance level provides a high degree of reliability of the claimed or declared identity of a give person and is characterized by referring to the corresponding technical specifications, standards and procedures, including their verifications, the purpose of which is to prevent misuse or identity changes. Evrotrust's electronic identification scheme, in terms of infrastructure, allows to generate, register and validate remotely unique electronic identities of natural persons and legal entities.

1.1. OVERVIEW

"Certificate Policy and Practice for Providing a Qualified Electronic Identification Service" ("the Policy"/CP-CPS-IdV/Certificate policy and practice for providing a qualified 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/advanced electronic signature whereby the statement with personal or other data is signed, remote signing of the statement with a qualified/advanced 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 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 it can 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 qualified 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);
- Law on electronic documents and electronic trust services;
- 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;
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) 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;
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 General requirements;
- 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 as part of the verification of the overall activity of the organization. The service is recognized by the national supervisory body as a qualified electronic identification service and is registered by the Communications Regulation Commission in the European Trusted List of qualified trust service providers.

1.3. POLICY NAME AND IDENTIFIER

The name of this document is: “Certificate Policy and Practice for Providing a Qualified 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/advanced electronic signature;
- Keeping the records (logs) for the electronic identification process, issuing qualified attribute certificates, and remote signing with a qualified/advanced electronic signature.

The profiles of all qualified operative certificates of the Certifying Authority issues are described in item 7 of the document "Certification Practice Statement for Providing Qualified Trust Services". The profiles of all user qualified certificates issued by the Operating Certifying Authority “Evrotrust

RSA Operational CA" are listed in item 7.5 of the document "Certification Practice Statement for Providing Qualified Trust Services".

1.4.2. REGISTERING AUTHORITY

The Registering Authority (RA) is a separate structure at Evrotrust, but can also be an external legal entity to which the company assigns the performance of registration, identification and identity certification services for natural persons and legal entities. Evrotrust's system for remote video identification is developed so as to enter a person's personal data in the system automatically, after scanning the identification document, but the identification process obligatorily goes through a verification by an operator of RA. If during the check of the video recording the operator has doubts concerning details of the process, he rejects and suspends the identification of the person or contacts them to clarify the procedure. The video conversations held by the operators are in line with internal procedures and built methodology. When the person experiences difficulties during the automated identification, they can initiate remote video identification with an operator from RA through their mobile device.

1.4.3. USERS

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

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

1.4.4. 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 service for the purposes of establishing business relations, professional, administrative, or other relations, or for the purposes of carrying out various operations or transactions. 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.

1.4.5. OTHER PARTICIPANTS

For certain activities, pursuant to Regulation (EU) No. 910/2014, Evrotrust may involve external parties. The relations regarding such activities shall be regulated in an agreement. Such agreement shall set out the rights and obligations of the external parties involved in the activity for providing electronic identification and trust services. Evrotrust uses subcontractors and service providers, such as specialized data centers, for reliable and secure colocation of server and network equipment, providers of cloud technologies and services, providers of automated identification services, IT services, provision of registration and authentication and others. When working with subcontractors and providers, Evrotrust requires them to strictly follow its procedures, in accordance with this Policy and Practice.

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. As a result of the provided high level of security, protection against unauthorised or unlawful processing, accidental loss, destruction or damage, the scope of the application of the electronic identification means far exceeds the boundaries of the Republic of Bulgaria. By notifying the electronic identification schemes and mutually recognizing the electronic identification means in the member-states a possibility is

provided to the citizens of the European Union to easily, quickly and lawfully use electronic administrative services.

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 AN ELECTRONIC IDENTIFICATION MEANS 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 Qualified Electronic Identification Service" is the CEO of Evrotrust.

Additional information may be received at the following address:

Evrotrust Technologies AD

1766 Sofia

251 G Okolovrasten Pat Av, MM Business Center, fl. 5

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:

“Electronic identification” means the process of using data in electronic format to identify persons whose data represent in a unique manner a given natural person or legal entity, or a natural person representing a legal entity;

“Electronic identification means” means a tangible and/or intangible unit containing identification data of persons, used to certify authenticity for an online service;

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

“Electronic identification scheme” means a system for electronic identification in which the electronic identification means are issued to natural persons or legal entities or natural persons representing legal entities;

"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 electronic register of Evrotrust is a repository holding current and previous versions of electronic documents (Policies and Practices, certificates by certifying authorities, and other information) to be used by users, relying parties 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 scheme for remote identification of natural/legal persons. The operating activities for providing an electronic identification service include issuing a qualified 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

The electronic identification scheme is a system for remote identification of natural persons and legal entities based on trust services regulated by Regulation (EU) No. 910/2014. Electronic identification is related to verification of personal and other data of natural persons, which data are included in the issued qualified attribute certificates, as well as in statements made by clients for providing personal and other data upon request by the relying party.

The scheme consists in two main processes: remote registration (onboarding) of a user and issuance of an identity certificate (identification service) to a user before relying parties.

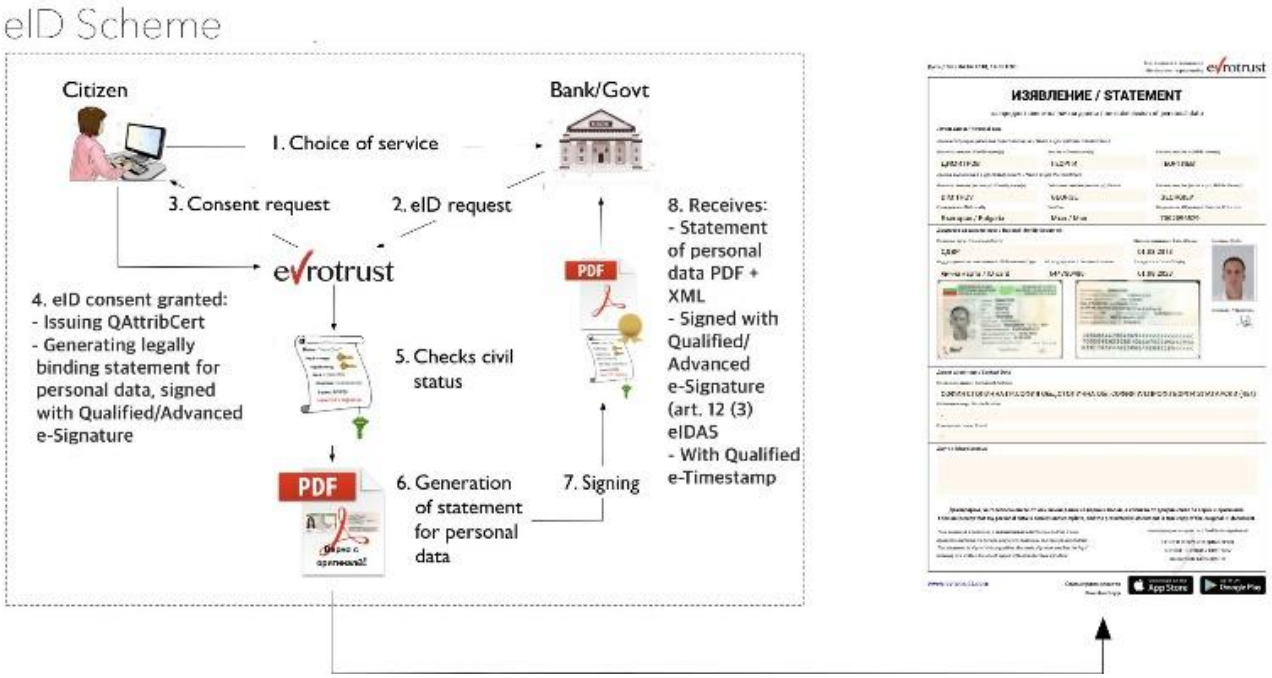
In order to start the remote registration process, it is necessary for the person to install Evrotrust's mobile application (independently or integrated, as an SDK module of a partner) on their cell phone. For the purposes of registration and subsequent identification, it is necessary that the person make a picture of their identification document with their cell phone camera and the data received from the machine-readable area of the ID document and the image are processed automatically, including verification for validity with a special software. The scheme is developed using a technology which recognised identification data automatically and sends them for certification to a reliable source (population register) using an inbuilt channel for connection in real time. In the case of a legal entity, the representation powers and identity data of the legal person are verified in the Commercial Register. When the identity document has incorporated biometric data and the device supports NFC technology, the data are extracted from there by placing near the mobile device. The automatic video identification process requires comparison of the picture of the face obtained from the identification document and the picture made by the mobile device camera in video recording regime. The obtained result comes from a high technology software which makes biometric analysis of the form and unique traits of the face. The process includes 3D verification for live object.

In order to identify a natural person who is the representative of a legal entity (managers, members of boards, procurators, etc.), when the representation authority is the result of a law, an automated verification is conducted in the respective registers when there is such integration (Commercial Register, Register of Non-profit Legal Entities and other).

In the case of unsuccessful automatic video identification (for example, due to possible changes of the face or the picture was not obtained from a reliable source) the process goes to video-identification by an Evrotrust operator. The video-session operator in real time visually identifies the person on the basis of a copy of the identity document and an extracted picture.

Every identification, independently of whether automated or performed by an operator, is subject to immediate subsequent human control. After successful identification of the person, a profile is created and they can be provided with a means of electronic identification and trust services.

The working mechanism of the electronic identification scheme includes the following key processes:



1. Issuance of a statement by the user with their personal data;
2. Generating a pair of keys for qualified/advanced electronic signature;
3. Issuance of a qualified attribute certificate of electronic signature possessing more than the standard minimum number of required attributes (personal data of the person);

4. Providing an instrument to the user to sign remotely with their private key the statement with the personal data;
5. The electronic identification means generated by the system (remotely signed statement by the user with their qualified/advanced electronic signature and with included additional attributes in the certificate) are provided to the relying party.

4.2. 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, remote signing 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 statement for providing personal data is accessible to the person in a readable PDF format through the mobile application or Evrotrust's signing portal, so that the person can read it before signing it. In the statement a working XML file is added with the same data in machine-readable format for automatic processing by the relying party.

The service provision process is initiated by a relying party which sends to 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. Each relying party representing an integrated partner of Evrotrust has the possibility to present a request by an Evrotrust user for identification. Evrotrust sends a message to the smart device of the person in the mobile application, with which it requests their consent for identification. The users of the electronic identification service are obliged to become familiar with an observe the General Terms and Conditions, the Contract, the Personal data protection policy, the Policies and Practices for providing electronic identification and trust services, the security measure related to the use of the electronic identification means and other documents published in the public electronic register of Evrotrust: https://www.evrotrust.com/landing/en/a/tsp-documents. The persons applying for the service cannot continue with their registration without becoming familiar with and accepting the requirements in the specified document. By activation a functionality in the mobile application the persons agree to the terms and conditions and sign a contract for services.

4.2.1. IDENTIFICATION OF A NATURAL PERSON

Evrotrust's remote system for video identification was developed in a way allowing the personal data of a natural person to be entered into the system automatically after scanning the national ID document held as proof of identity. The verification of the validity of the ID document is performed using automated checks through the national database for ID documents and goes through several controls. Officially recognized documents in the country of origin are accepted as valid – international passport, diplomat passport, sailor passport, foreigner's personal ID card, driver's license and other documents, in line with the national legislation of the citizen of the respective country.

The minimum amount of data the relying party can request from Evrotrust's user for the purposes of verifying the identity of the natural person are:

- last name (or names),
- first name (or names),
- date of birth,
- unique national identifier, if any, in line with the technical specifications, for the purposes of cross-border identification, which remains unchanged for as long as possible (for example, in the Republic of Bulgaria it is PIN/FIN),
- cell phone number and
- e-mail address.

Additional specific data which can be presented are:

- first name (or names) and last name (or names) at birth,
- place of birth,
- permanent address and
- sex.

Evrotrust reserves the right, depending on the realization of the integration with the different types of ID documents, primary registers and reliable sources of data, to supplement the specific data set.

4.2.2. CERTIFICATION OF THE IDENTITY OF A LEGAL ENTITY

For a legal entity or natural person that represents it (managers, members of boards, authorized signatories, etc.), when the representative authority results from a law, remote verification and collection of the data on the legal entity is performed in the official public registers (for example, in Bulgaria the verification is made in the registers of the Registry Agency). The verification is made on the basis of a unique national identifier recorded in Evrotrust's application, according to the technical specifications for the purposes of cross-border identification, which remains unchanged for as long as possible (for example, in the Republic of Bulgaria this is UIC/BULSTAT). Evrotrust verifies the proof in a reliable source (when there is integration), in order to establish whether it is authentic or known as existing and to bring to a minimum the risk the identity of the legal entity to not correspond to the stated identity, taking into account the risk the respective documents to have been lost, stolen, with terminated validity, revoked or with expired validity. The purpose of the verification of the identity of the legal entity is to prove that, at the time of the review of the request to issue a qualified certificate, the legal entity exists and that the representing person applying for the service for the issuance of electronic identification means has representation powers to request the issuance. An identity check is performed for the natural person, in line with the above paragraph.

To the minimum data set for a legal entity additional specific data can be added, for one or more of the following elements: current address, VAT registration number; tax number.

Depending on the implemented integration with primary registers and reliable data sources, Evrotrust can supplement the additional data set for legal entities.

4.3. ELECTRONIC IDENTIFICAITON MEANS

The electronic identification means according to Evrotrust's electronic identification scheme, meets the requirements of art. 3, para. 2 of Regulation (EU) 910/2014. It contains data for the identification of the person and consists of: PDF+XML document containing persona identification data of the person, including graphic elements, such as a copy of the ID document, image of the signature, picture, etc.; qualified/advanced electronic signature of the signed PDF/XML document; and attribute qualified certificate linked with the qualified/advanced

signature, containing all personal data which can be listed in the certificate, according to standard X.509 (for example the graphic elements cannot be listed).

The electronic identification means is generated at the request of the end user in real time, including the generation of a pair of keys, a qualified/advanced certificate is issued and a remote signature is created (remote signing is carried out). The electronic identification means is provided automatically to the relying party for certification of an online service. The relaying party can extract the information both from the PDF/XML document and from the attribute qualified certificate and can trust the identity data of the person, in accordance with Regulation (EU) No. 910/2014.

The electronic identification means is protected from duplicating and falsifying by using cryptographic keys and algorithms. The protection against high-potential attackers is carried out through complete measures, including DDOS defence systems, firewalls, reservation systems and many other software and hardware solutions. In this sense, it can be assumed that the electronic identification means is used only under the control or held by the person to whom it belongs. The mobile application used was designed so that the person to whom it belongs can protect it reliably against use by other persons using access codes, facial and finger biometric data and other protection means. All of this is activated and regulated by the person.

4.3.1. ISSUANCE, PROVISION AND ACTIVATION

The electronic identification means is provided to the relying party through an API channel. During the entire process the session is encrypted by cryptographic keys provided by the persons responsible for the relying party. The verification of the status of the relying party is made with all possible means.

The issuance of the electronic identification means is an automated process which is carried out after successful identification of the person. In order to activate the issuance process, at least a two-factor certification is required. the means is activated when issued.

The qualified attribute certificates issued by Evrotrust's Certifying Authority "Evrotrust RSA Operational CA" meets the requirements of Regulation (EU) 914/2014 and are recognized in the European Union. In view of the operative cross-border compatibility of the qualified electronic signatures introduced with Regulation (EU) No. 910/2014, the qualified attribute certificates do not exceed the required requisites provided in Regulation (EU) No. 910/2014 and Regulation (EU)

2015/1501[1] concerning the requirements for the minimum data set to identify persons which represents in a unique manner a given natural or legal person.

The relying party receives through an interface agreed 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.

4.3.2. TEMPORARY SUSPENSION OF THE VALIDITY, REVOCATION AND REACTIVATION

The temporary suspension of the validity, cancellation and reactivation of the electronic identification means is related to the management of the person's account at Evrotrust. It is applied for the issued certificates of an advanced/qualified electronic signature of the person and is related to their management. Their management provides a temporary HOLD, cancellation (REVOKE) or deletion of the private keys related to the certificates and reactivation (RESTORE).

At any time, the mobile application user can manage (temporarily suspend and subsequently restore) their account, being able to deactivate it and subsequently activate it using the respective functionality. This allows to generate/cancel electronic identification means. When a functionality is activated through the mobile application for account deletion, but after some time the person decides to obtain trust services, this person has to undergo a new registration and identification process.

After temporary suspension, the person can reactivate their account again by meeting the same security requirements as those established before the suspension or cancellation. The reactivation restores the person's ability to identify themselves before third parties by generating electronic identification means.

The management of the electronic identification is entirely under the control of the person who owns the data from their mobile device. Each change is subject to a two-factor certification mechanism.

[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*

4.3.3. RENEWAL AND REPLACEMENT

At any request for identification of the person the system checks the validity of the data in real time (for example, the validity of the ID document, the validity of the data in the primary registers, etc.) and, in the event of changes, the data are updated, so that the electronic identification means are generated with updated data. Evrotrust actively monitors for changes and, if there are such changes, it requests from the person to identify themselves once again. If the changes are identified (for example, the ID document has expired or new data have been registered in the primary registers), an initial identification process is activated which meets the same security requirements as the initial proof and check of identity. The personal data are processed in a manner guaranteeing a high level of security, including protection against unauthorized or illegal processing, as well as against accidental loss, destruction or damage, by applying suitable technical and organizational measures. Evrotrust checks the personal data against a reliable source or using an NFC chip integrated into the document.

4.4. SUSPENSION OR CANCELLATION OF THE SCHEME OR MEANS FOR ELECTRONIC IDENTIFICATION

The electronic identification scheme represents and integral part of the infrastructure of Evrotrust's technological system for the provision of remote trust services. In this sense, Evrotrust can suspend or cancel the validity of the scheme in the event of: termination of the overall activity of the organization or the certifying body; declaring bankruptcy; due to end of the life-cycle or decommissioning of a hardware or software element used to provide electronic identification; in the event of compromising or suspicion of compromising a private key; in the event of a disaster or serious problem which do not allow satisfactory restoration of the electronic identification service.

Evrotrust can terminate immediately an attribute certificate issued by it with which the personal data statement is signed in the event of: death or incapacity mandate for a natural person or with the termination of the representation powers of the legal entity; upon establishing false data when issuing the certificate; upon changes in already certified information; when the private key or PIN code have been compromised; loss of a mobile device; malicious actions; delay in the payment of the remuneration due; request to terminate on the part of the person.

Evrotrust's mobile application provides every user with the possibility to deactivate the electronic identification means by activating the respective functionality. By activating the account termination functionality in the application, also the contract for providing electronic identification services is terminated. The terminated identification cannot be renewed, but a new one can be requested. Each user can request suspension or termination of an attribute certificate through the mobile application without an identity check.

A request to terminate or revoke the entire identification scheme, as well as to suspend or terminate certificates issued by Evrotrust to natural persons or legal entities with which the statements for provision of personal data are signed, can be received from the Communications Regulation Commission or a state organization with powers in line with the national legislation.

4.5. IDENTIFICATION AND VERIFICATION OF IDENTITY AFTER ACCOUNT TERMINATION

When a functionality is activated through Evrotrust's mobile application for the deletion of a profile and upon request by a given person to provide identification services later on, they have to go through a new registration and identification process.

4.6. REQUIREMENTS RELATED TO THE INTEROPERABILITY

Article 12 of Regulation (EU) No. 910/2014 (Cooperation and interoperability) provides the national electronic identification schemes for which notification is made according to art. 9, para. 1 to interact and this to impose the creation of an interoperability framework. Evrotrust's electronic identification scheme was built according to the requirements of Regulation (EU) 2015/1501 concerning technical and operative requirements, so as to guarantee the interoperability with the other electronic identification schemes for which notification is sent to the Commission by the member states.

Evrotrust possesses certification by a Conformity assessment body pursuant to Regulation (EU) No. 2015/1502, which establishes fulfilment of the requirements of art. 4 of Regulation (EU) No. 2015/1501 concerning the categorization of the national assurance levels of the notified electronic identification schemes to be performed according to the requirements established in Regulation (EU) No. 2015/1502 and the conformity with the "high" assurance level for electronic identification means defined in art. 8 (2) of Regulation (EU) No. 910/2014.

Evrotrust's electronic identification service is provided according to a methodology for the identification of persons which meets the requirements of art. 11 of Regulation (EU) No. 2015/1501 for the collection of a minimum personal data set which unequivocally will represent a natural or legal person. The minimum data set for a natural person includes: last name (or names), first name (or names), date of birth, national unique identifier, if any, in line with the technical specifications for the purposes of cross-border identification, which will remain unchanged as long as possible, cell phone number and e-mail. For a legal entity and for a natural person – its representatives (managers, board members, authorized signatories, etc.), when the representing authority results from a law, a remote check is conducted on the basis of a unique national identifier recorded in Evrotrust's application in line with the technical specifications for the purposes of cross-border identification, which remains unchanged for as long as possible.

The electronic identification scheme was implemented according to Regulation (EU) No. 910/2014 and the technical specifications developed according to it. In the "Practice in providing qualified trust services" of Evrotrust and in the "Policy and practice in providing the qualified service for the issuance of attribute certificates", the profile of the attribute qualified certificate is described, which certificate is a part of the electronic identification means and is in line with the requirements of the standards: ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3 and ETSI EN 319 412-5. Evrotrust provides means for electronic identification in line with the above and all other technical specifications and recommendations related to the technology developed by the organization and fulfilling the requirement of Regulation (EU) No. 2015/1501 for the purposes of interoperability.

In connection with the mechanisms for dispute settlements, as specified in art. 13 of Regulation (EU) No. 2015/1501, within the context of interoperability, Evrotrust has a procedure for submitting, reviewing and resolving suggestions, complaints, signals and claims received from users, clients or relying parties concerning the provision of the services or other matters related to them. (See item 21 of this document).

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 items 6.5 and 6.6 of the document named "Certification Practice for Providing Qualified Trust

Services".

5.1. PREMISES AND PREMISES STRUCTURE

Evrotrust has specially designed and equipped premises with the highest degree of physical access control, in which the Certifying Authority of Evrotrust as well as all central components of the infrastructure are housed.

The description of the premises and the related supporting systems is contained in item 5.1 of the document "**Certification** *Practice for Providing Qualified Trust Services*".

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. Evrotrust has placed its critical infrastructure in two cabinets certified according to all requirements for this category of storage equipment in two specially built and isolated rooms, in two data centers. 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. 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 item 5.1.2 of 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.

The work process with carriers is described in item 5.1.7 of the document "Certification Practice for Providing Qualified Trust Services".

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 with appropriate technical devices. This applies to carriers which do not allow for stored data to be permanently destroyed and to be reused. In specific cases, the information from portable carriers is destroyed through deletion or formatting of the device, without any option for recovery.

The measures related to the waste disposal process is described in item 5.1.8 of the document "Certification Practice for Providing Qualified Trust Services".

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 a sufficient number of qualified employees so that, at any time during the performance of its activities, such employees can ensure compliance with the legislation in force and with the internal rules and regulations of the company.

The procedure is described in item 5.2 the document "Certification Practice for Providing Qualified Trust Services".

7. EVENT RECORDINGS AND KEEPING DIARIES

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.

Diaries 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.

The procedure for the management of records and keeping diaries is described in item 5.4 of the document "Certification Practice for Providing Qualified Trust Services".

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 "Information Security Policy" of Evrotrust, an analysis is carried out of the vulnerability assessment for all internal procedures, applications and information systems. Analytical requirements can also be established 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.

The measures related to the assessment of vulnerability are described in item 5.4.8 of the document "Certification Practice for Providing Qualified Trust Services".

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 Bodies and by the Registration Body; 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.

The archiving procedure is described in item 5.4.8 of the document "Certification Practice for Providing Qualified Trust Services".

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 continuity of the issuance of electronic identification means and qualified trust services for users, Evrotrust may sign an agreement with another qualified trust service provider. In such case, Evrotrust:

- notifies the Supervisory Body 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 assumes Evrotrust's rights, obligations and the archive.
- The receiving provider takes over the rights, obligations and the archive of Evrotrust.

10.3. REVOCATION 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 item 6 of 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 item 6.5 of 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 item 6.6 of 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 item 6.7 of the document "Certification Practice for Providing Qualified Trust Services".

13. AUDITS AND CONTROL OVER THE ACTIVITY OF EVROTRUST

The procedure is described in item 8 of the document "Certification Practice for Providing Qualified Trust Services".

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 implemented integrated management system 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.

[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*

13.2. INDEPENDENT EXTERNAL AUDIT

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 months by an independent audit team according to 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

In accordance with art. 32 of the Law on electronic documents and electronic certification services (LEDECS), the Communications Regulation Commission (CRC) is the National Supervisory Body in the area of electronic trust services exercising the powers under art. 17 of Regulation (EU) No 910/2014. CRC provides and revokes qualified status to the providers of trust services and the services provided with them, pursuant to art. 20 and 21 of Regulation (EU) No 910/2014. The supervisory body creates, maintains and publishes the national trusted list of the persons providing trust services and qualified trust services, according to art. 22 of Regulation (EU) No 910/2014. To exercise it functions, CRC has the right of free access to the sites subject to control; to verify the qualification documents of the employees of trust service providers; to require information and documents related to the implementation of control; to establish persons-bodies for the assessment of compliance pursuant to art. 33 LEDETS who carry out audits for compliance by the providers of qualified trust services with the requirements of art. 21, para. 1 and 2 LEDECS; to obtain from the provides of trust services the information needed for the implementation of its powers.

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.

Evrotrust concludes a compulsory insurance contract for 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.

15. 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.

The rules for complying with the inviolability of personal data is described in item 9.4 of the document "Certification Practice for Providing Qualified Trust Services".

15.1. 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.

The issue about the possession of intellectual property rights is described in item 9.5 of the document "Certification Practice for Providing Qualified Trust Services".

16. LIABILITIES, RESPONSIBILITY AND GUARANTEES OF EVROTRUST

16.1. 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 and European legislation in the performance of its activity as a Provider of Qualified Trust Service and electronic identity;
- 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 and issuing an electronic identification means 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 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 of their obligations and due diligence while using the trust services provided by Evrotrust, and of the proper and safe use of the issued attribute certificates and the provided electronic identification means;
- using and storing the collected personal and other type of information solely for the purposes of its activity for providing electronic identification and qualified certificates, in accordance with the national and European legislation;
- 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 a public electronic register/repository;
- providing continuous access to the Public Electronic Register (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 every relying party to verify the status of an issued and published attribute certificate in the electronic 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;
- it has implemented an electronic identification scheme in accordance with Regulation (EU) No. 941/2014 and the technical specifications developed in relation to it;
- complying with the requirements of ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5 when creating the account of the attribute qualified certificate which is a part of the electronic identification means;
- Evrotrust provides electronic identification means in line with ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5 and all other technical specifications and recommendations related to the technology developed by the organization and in implementation of the requirements of Regulation (EU) No. 2015/1501 for the purposes of

interoperability;

- in order to settle any disputes arisen, Evrotrust uses and internal procedure for the submission, review of resolution of suggestions, complaints, signals and claims received from users, clients and relying parties concerning the provision of the services or other related issues.
- maintaining, on the website of Evrotrust, a list of registration bodies, a list of recommended software and hardware for users, also forms, templates, a standard contract, and other documents for the benefit of users.

16.2. 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 910/2014 and Regulation (EU) No. 2016/679 in carrying out its activity of providing electronic identification and trust services;
- from untrue or missing data in the qualified attribute certificate as at the time of its issuance;
- from algorithmic incompatibility between the private and the public key recorded in the certificate;
- from failure to comply with its obligations to issue and manage qualified attribute certificates;
- from omissions in establishing the person's identity.

17. OBLIGATIONS OF USERS

The users of the identity verification service which includes the issuance of electronic identification means and the qualified attribute certificates related to them 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 in the other documents published in the Evrotrust Public Electronic 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.

18. 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.

19. 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.

20. DISPUTE RESOLUTION

Evrotrust has a procedure for submitting, reviewing and resolving suggestions, complaints, signals and claims received from users, clients or relying parties concerning the provisions of the services or other related matters.

Only dissimilarities or contradictions between parties which are parts to the contract to

Evrotrust can be the subject to disputes. Disputes or complaints concerning the use of certificates, electronic identification means and trust services provided by Evrotrust will be settled through mediation on the basis of information submitted in writing. Each complaint has to include a description of the topic, the cause or circumstances related to the problem which cause it, as well as the full name, address, e-mail and contact telephone of the applicant. Copies of documents related to the described topic may be attached to the submitted complaints.

When a claim is brought, the user has to specify its subject, the preferred manner of settlement of the claim, respectively, the required amount of money, and contact address. When submitting a claim, the user must also provide the documents on which the claim is based. When a claim is brought for the services, the user can request the service to be performed in accordance with the contract, a rebate or reimbursement of the amount paid.

The submission of complaints, signals or claims shall be made in the following manner:

- in person, in writing on paper, and signed by hand (as an exception, oral submission is allowed only and solely for claims), in the office at the address:

Evrotrust Technologies JSC

city of Sofia, 1766

251 G Okolovrasten pat Av, MM BUSINESS CENTER, fl. 5

telephone, fax: + 359 2 448 58 58

e-mail: office@evrotrust.com

- to Evrotrust's e-mail address (office@evrotrust.com or dpo@evrotrust.com;), signed with a qualified electronic signature.

Evrotrust shall review each complaint or claim received and prepare a written response within 7 days with suggestions for the actions to take (if applicable). When for the resolution of a specific complaint or claim it is necessary to collect additional information for the case, requiring more time, the applicant shall be notified in writing, setting out the respective motives. Evrotrust shall review any complaint or claim received and send a final response to the applicant within 1 (one) month.

21. APPLICABLE LAWS

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

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.