

**CERTIFICATE POLICY AND PRACTICE  
FOR PROVIDING A QUALIFIED ELECTRONIC IDENTIFICATION  
SERVICE VIA WEB INTERFACE**

## CONTENTS

1.	INTRODUCTION.....	4
1.1.	OVERVIEW.....	5
1.2.	COMPLIANCE .....	6
1.3.	POLICY NAME AND IDENTIFIER.....	7
1.4.	PARTICIPANTS IN THE INFRASTRUCTURE .....	7
1.4.1.	REGISTERING AUTHORITY .....	7
1.4.2.	USERS .....	8
1.4.3.	RELYING PARTIES .....	8
1.4.4.	OTHER PARTICIPANTS .....	9
1.5.	APPLICABILITY AND USE OF ELECTRONIC IDENTIFICATION VIA WEB INTERFACE .....	9
1.5.1.	APPLICABILITY OF THE SERVICE .....	9
1.5.2.	USE OF THE ELECTRONIC IDENTIFICATION SERVICE VIA WEB INTERFACE.....	9
1.5.3.	ACCEPTING AN ELECTRONIC IDENTIFICATION MEANS BY RELYING PARTIES.....	9
1.5.4.	PROHIBITION ON THE USE OF THE ELECTRONIC IDENTIFICATION SERVICE VIA WEB INTERFACE .....	10
1.5.5.	LIMITATIONS ON USING THE ELECTRONIC IDENTIFICATION SERVICE VIA WEB INTERFACE .....	10
1.6.	MANAGEMENT OF THE POLICY AND OF THE PRACTICE.....	10
2.	DEFINITIONS.....	11
3.	PUBLIC REGISTER.....	12
4.	OPERATING ACTIVITIES FOR PROVIDING AN ELECTRONIC IDENTIFICATION SERVICE VIA WEB INTERFACE.....	12
4.1.	PRINCIPAL SCHEME .....	12
4.1.1.	PROCESS OF THE ELECTRONIC IDENTITY AUTHENTICATION VIA WEB INTERFACE.....	13
4.1.2.	PROCESS OF ISSUING A QCQES / QCAES AFTER VERIFICATION OF ELECTRONIC IDENTITY THROUGH WEB INTERFACE .....	14
4.2.	AUTHENTICATION PROCEDURE.....	15
4.2.1.	IDENTIFICATION OF A NATURAL PERSON.....	16
4.2.2.	CERTIFICATION OF THE IDENTITY OF A LEGAL ENTITY .....	17
4.3.	ELECTRONIC IDENTIFICATION MEANS.....	18
4.3.1.	ISSUANCE, PROVISION AND ACTIVATION.....	18
4.3.2.	TEMPORARY SUSPENSION OF THE VALIDITY, REVOCATION AND REACTIVATION .....	18
4.3.3.	RENEWAL AND REPLACEMENT .....	19
4.4.	SUSPENSION OR CANCELLATION OF THE SCHEME OR MEANS FOR ELECTRONIC IDENTIFICATION.....	19
4.5.	REQUIREMENTS RELATED TO THE INTEROPERABILITY .....	19
5.	PHYSICAL SECURITY CONTROL .....	20
5.1.	PREMISES AND PREMISES STRUCTURE.....	20
5.2.	PHYSICAL ACCESS.....	21
5.3.	STORAGE OF DATA CARRIERS.....	21
5.4.	WASTE DISPOSAL.....	22
6.	ORGANIZATIONAL CONTROL .....	22
7.	EVENT RECORDINGS AND KEEPING DIARIES .....	22
8.	VULNERABILITY AND ASSESSMENT.....	23
9.	ARCHIVING .....	23
10.	TERMINATING THE ACTIVITIES OF EVROTRUST.....	24
10.1.	TERMINATING THE ACTIVITY OF A CERTIFYING AUTHORITY .....	24

10.2.	TRANSFER OF ACTIVITY TO ANOTHER QUALIFIED TRUST SERVICE PROVIDER .....	24
10.3.	REVOCATION OF THE QUALIFIED STATUS OF EVROTRUST .....	25
11.	MANAGEMENT AND CONTROL OF TECHNICAL SECURITY .....	25
12.	COMPUTER SYSTEMS SECURITY .....	25
12.1.	TECHNOLOGY SYSTEM LIFECYCLE SECURITY .....	26
12.1.	NETWORK SECURITY .....	26
13.	AUDITS AND CONTROL OVER THE ACTIVITY OF EVROTRUST .....	26
13.1.	INTERNAL AUDITS .....	26
13.2.	INDEPENDENT EXTERNAL AUDIT .....	27
13.3.	AUDIT BY THE NATIONAL SUPERVISORY BODY .....	27
14.	FINANCIAL RESPONSIBILITIES.....	28
15.	INVOLABILITY OF PERSONAL DATA .....	28
15.1.	INTELLECTUAL PROPERTY RIGHTS .....	28
16.	LIABILITIES, RESPONSIBILITY AND GUARANTEES OF EVROTRUST .....	29
16.1.	GUARANTEES AND LIABILITIES.....	29
16.2.	RESPONSIBILITIES .....	30
17.	OBLIGATIONS OF USERS .....	31
18.	RESPONSIBILITY OF THE USER.....	31
19.	DISCLAIMER.....	31
20.	DISPUTE RESOLUTION .....	32
21.	APPLICABLE LAWS.....	33

## 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: 251G Okolovrasten pat Str., Business center MM, floor 5, 1766 Sofia, Bulgaria, 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 trust service of electronic identification through a web interface. Electronic identification is a process using data in electronic format to identify persons whose data represent in a unique manner a given natural person, a natural person representing a legal entity, or a legal entity. Electronic identification provides citizens with the possibility to access online services, their legal security and possibility for easy interaction among business, public bodies and citizens. The service allows for a reliable and secure user identification, offering users a possibility for secure authentication of their identity before relying parties. Among the advantages of the provided service is identification at any place and any time. Evrotrust's innovative decision to develop and provide an identification scheme through a web interface is related to the extremely powerful development and popularization of the worldwide web of browsers. In the modern world, access to information resources and electronic services through a browser is the most used, universal, fast and convenient way for citizens. Using a qualified service for electronic identification via web interface is in full compliance with the legislation in force and Regulation (EU) No. 910/2014.

Evrotrust's 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 secure and reliable method for remote certification and verification of the identity of citizens. The means of electronic identification that Evrotrust provides to the persons (respectively to the relying parties) contains their identification data and is used for authentication for using an online service. The means is certified in accordance with Regulation (EU) No. 2015/1502 for "high" level of assurance, and depending on the specific implementation by the relying parties, it can be provided to users with a level of assurance of "high", "significant" or "low". The assurance level provides a sufficient 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.

This service allows to unambiguously verify and authenticate the electronic identity of individuals and legal entities (in the presence of developed functionality for legal entities) remotely, through a mobile or stationary (computer) device with a standard web browser installed.

## **1.1. OVERVIEW**

"Certificate Policy and Practice for Providing a Qualified Electronic Identification Service via Web Interface" ("the Policy"/CP-CPS-WebID/Certificate policy and practice for providing a qualified electronic identification service via web interface) is a document describing the general rules and standards applied by 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 and means which contain such data. This document describes the general requirements for provision of the electronic identification service through web interface, as well as the security measures, rights and obligations for all stakeholders, including certifying authorities, corporate clients, end users and relying parties. The service provides a secure and reliable identification method within the meaning of Article 24, Para. 1, item (d) of Regulation (EU) No. 910/2014, providing a level of assurance equivalent in terms of reliability to physical presence.

This document forms an inseparable part of the General Terms and Conditions of the Contract for Trust, Information, Cryptographic and Other Services of Evrotrust (the General Terms and Conditions / GTC). 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>.

## 1.2. COMPLIANCE

Certificate policy and practice for providing a qualified electronic identification service via web interface 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 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 via Web Interface”, with object identifier (OID): 1.3.6.1.4.1.47272.2.16.17.4.

### **1.4. PARTICIPANTS IN THE INFRASTRUCTURE**

#### **1.4.1. 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. The system for remote video identification via web interface is developed so as to enter a person’s personal data in the system automatically, after scanning the identification document, but the identification process may go through a video conference call and/or verification by an operator of RA. If during the check of the video recording the operator has doubts concerning details of the process, he/she contacts the person to clarify the issues and/or contacts the relying party to notify them. 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 the device used.

### **1.4.2. USERS**

Any natural or legal person who has concluded a contract with Evrotrust for qualified electronic identification service through a web interface, as well as any person who has requested remote issuance of a qualified or advanced certificate after such identification, in cases where a relying party has integrated such functionality for the purpose of one-time signing of a contract or other documents with the person, is a user of this service.

When this is practically possible, the provided trust service is also accessible 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 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 electronic register of certificates that Evrotrust uses in its activities, to the issued user certificates, as well as to the certificate revocation list (CRL). Evrotrust provides a service for checking the status of issued certificates, when such are issued, in real time in an automated, reliable, free and efficient way. This service is made available at any time and even after the validity period of the certificates, based on the Online Certificate Status Protocol (OCSP). Any relying party, when accepting a qualified certificate, can check its status in real time. Evrotrust provides a service for qualified validation of qualified electronic signatures and seals in an automated and reliable way. As a result of the validation process, the service prepares a detailed report, which describes the status, reason, date and time of the provided status, as well as additional data. The service ensures that signatures/seals are created and verified in accordance with European legislation.

#### **1.4.4. 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 VIA WEB INTERFACE**

#### **1.5.1. APPLICABILITY OF THE SERVICE**

The applicability of the electronic identification service via web interface is related to easy quick and reliable authenticating of personal and other data of natural and legal persons, when functionality for legal persons is available, using a standard browser, such data being provided in documents with structured contents in a format defined by Evrotrust. 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 issued by Evrotrust far exceeds the boundaries of the Republic of Bulgaria.

#### **1.5.2. USE OF THE ELECTRONIC IDENTIFICATION SERVICE VIA WEB INTERFACE**

Users can use the means issued by Evrotrust with authenticated data once, in real time, at the request of a relying party.

#### **1.5.3. ACCEPTING AN ELECTRONIC IDENTIFICATION MEANS BY RELYING PARTIES**

Relying parties shall accept the authenticated persons' data for the specific assurance levels of the means of electronic identification through a web interface related to the Evrotrust identification scheme. Evrotrust does not bear responsibility if the relying party does not have the necessary information about the service provided, does not carry out checks on the method

of electronic identification and the level of assurance of the received means with authenticated data, does not have the right to process personal data of persons or processes them in violation of applicable and European legislation.

#### **1.5.4. PROHIBITION ON THE USE OF THE ELECTRONIC IDENTIFICATION SERVICE VIA WEB INTERFACE**

The electronic identification service shall not be used in a way which may lead to a breach of user personal data confidentiality, integrity and security. The Service must not be used inconsistently with the requirements of this document and in any other illegal way of application.

#### **1.5.5. LIMITATIONS ON USING THE ELECTRONIC IDENTIFICATION SERVICE VIA WEB INTERFACE**

The electronic identification service through a web interface as a stand-alone service is intended for transactions of up to EUR 5,000 (five thousand euro). The liability of the service provider under Regulation (EU) No. 910/2014 is limited to this limit. In the presence of an issued QCQES/QCAES based on the identification carried out through the web interface, the applicable limit of liability is specified in the issued qualified certificate. Use and reliance on the service output for other purposes is at the risk and responsibility of the respective relying parties.

### **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 via Web Interface" is the CEO of Evrotrust.

Additional information may be received at the following address:

Evrotrust Technologies AD

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

1766 Sofia, Bulgaria

Phone number: + 359 2 448 58 58

E-mail: [office@evrotrust.com](mailto: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 or advanced 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.

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

### **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.

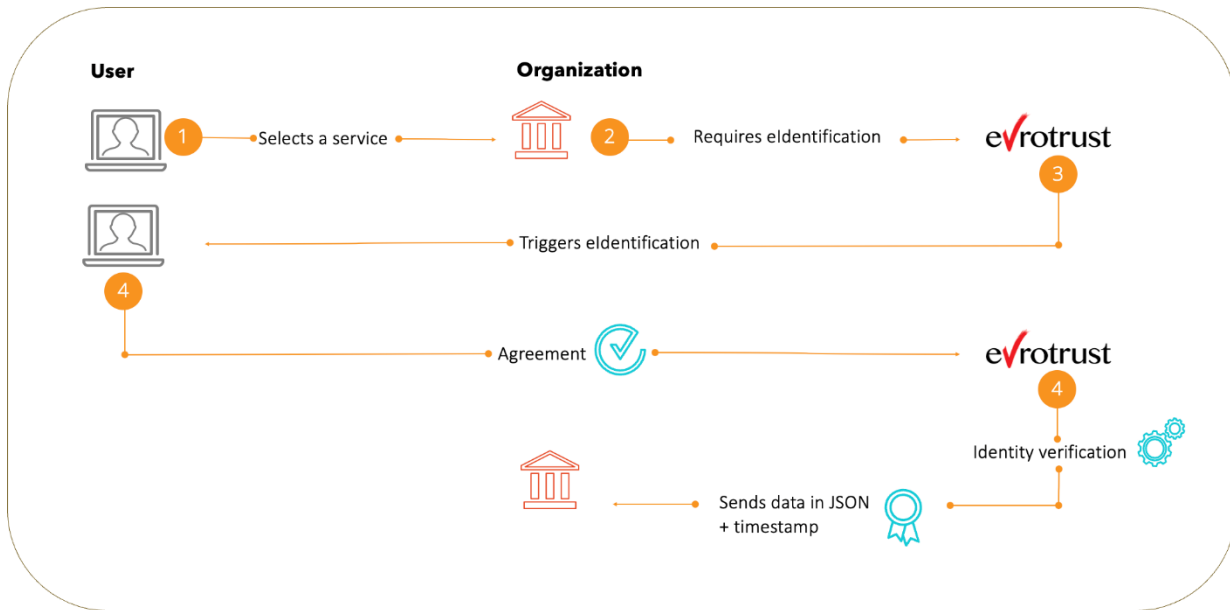
## **4. OPERATING ACTIVITIES FOR PROVIDING AN ELECTRONIC IDENTIFICATION SERVICE VIA WEB INTERFACE**

### **4.1. PRINCIPAL SCHEME**

Evrotrust verifies the identity of a person by using a method for remote identification of natural/legal persons. The operating activities for providing an electronic identification service via web interface include issuing a document in a structured format containing personal data and its delivery to a relying party at the request of a Evrotrust user. Evrotrust guarantees that the person has been identified by the system and that the data contained in the document provided to the relying party correspond to those contained in the personal identification document presented by the person. 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 a relying party (such as a bank, an insurance company, etc.) via a specially developed communication interface.

The main processes of the scheme and the electronic identification service through a web interface are described in the following scheme:



#### 4.1.1.PROCESS OF THE ELECTRONIC IDENTITY AUTHENTICATION VIA WEB INTERFACE

The electronic identification scheme used is a system for remote identification of natural persons and legal entities via web interface is full compliance with Regulation (EU) No. 910/2014. Electronic identification is related to collection, processing, checking and verification of personal and other data of natural persons upon request by the relying party.

In order to start the remote identification process, it is necessary for the person to open a web page in a previously known and supported browser in which Evrotrust's remote electronic identification solution via a web interface is integrated. Evrotrust can implement various technologies that meet the requirements described in this policy. For the purposes of registration and subsequent identification, it is necessary that the person make a picture of their identification document with the camera of the device used 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 (register of

personal identification documents) using an inbuilt channel for connection in real time (where integration is available). In the case of a legal entity, the representation powers and identity data of the legal person are verified in the Commercial Register or other applicable register, where respective access is available. When the identity document has incorporated data in an ICAO chip and the device supports NFC technology, the data are extracted from there by placing near a mobile device, where the solution supports such functionality. The automatic video identification process requires comparison of the picture of the face obtained from the identification document and the picture made by the device camera in video recording regime. The obtained result is generated by 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, low resolution, low quality of the recording, etc.) the process goes to video-identification by an Evrotrust operator. During the video conference call the operator visually identifies the person and on the basis of a comparative analysis of the identity document and the photograph extracted from it, verifies the person and confirms the data.

Every identification, independently of whether automated or performed by an operator, may be subject to subsequent human control following a standard methodology. After successful identification of the person and validation of the data collected about them, a structured data file, is provided over a secure channel to the relying party, over an Internet connection, with a text-based open standard for human-readable data exchange.

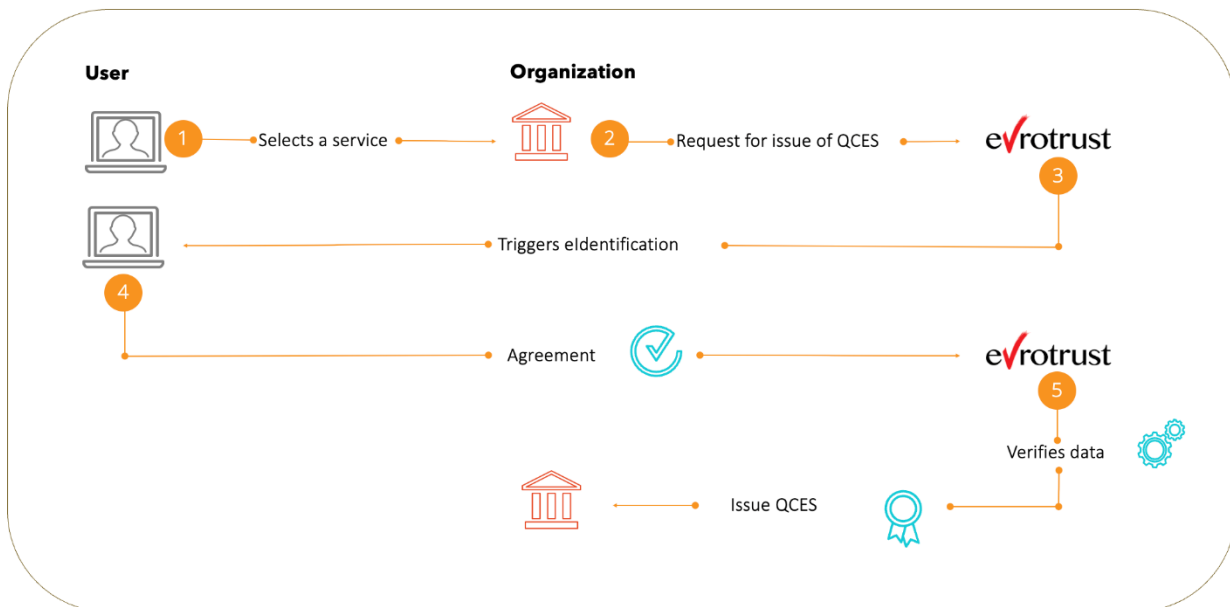
#### **4.1.2.PROCESS OF ISSUING A QCQES / QCAES AFTER VERIFICATION OF ELECTRONIC IDENTITY THROUGH WEB INTERFACE**

The identification carried out according to the method described in item 4.1 can also be used for the purposes of issuing a certificate for a qualified or advanced electronic signature (QCQES / QCAES). In these cases, after the successful identification of the person, the authenticated data is used to provide the corresponding trust service. The issuance of the QCQES

/ QCAES may follow the identification of the person in time, in which case the validity of the identification data must be verified again before issuing the certificate.

As far as this document does not provide otherwise, for the issuance of QCQES / QCAES after applying the method of performing identification through a web interface described in this document, the documents *Certificate policy for qualified certification services for qualified electronic signature/seal*, *Certificate policy for qualified certification services for advanced electronic signature/seal* and *Certification practice statement for qualified trust services* shall apply.

The mechanism of operation of the electronic identification scheme via web interface for the purpose of issuing QCQES / QCAES covers the following key processes:



## 4.2. AUTHENTICATION PROCEDURE

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 create a document with structured contents, containing their personal data.

The service provision process is initiated by the natural person requesting to be identified by a relying party by activating the respective functionality of the web interface provided. Apart from Evrotrust, each relying party representing an integration partner of Evrotrust has the possibility to integrate and provide to persons the software and technical means and web interface for using the service. The users of the electronic identification service via web interface

are obliged to become familiar with and observe the General Terms and Conditions of Evrotrust, 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>. The persons requesting use of the service cannot continue with their identification without becoming familiar with and accepting the requirements in the specified documents using the functionality for acceptance thereof provided in the respective web interface. By activating this functionality the persons agree to the terms and conditions and sign a contract with Evrotrust to provide the service according to the General Terms and Conditions, and Evrotrust activates the functionality for remote identification before the relevant party that provided the web interface.

#### **4.2.1. IDENTIFICATION OF A NATURAL PERSON**

The 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 a reliable proof of identity. The verification of the validity of the ID document is performed using automated checks through the national database for ID documents (where such connectivity is available) and goes through a number of controls. Officially recognized documents in the country of origin are accepted as valid – international passport, diplomat passport, sailor passport, ID card and other documents, in line with the national legislation of the issuing country.

The minimum amount of data the identified person can request Evrotrust to provide to the respective relying party for the purpose of their identification before it 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),
- personal ID document number.

Additional specific data which can be presented are:

- first name (or names) and last name (or names) at birth,
- place of birth,
- permanent address;
- sex;
- date of issue of personal ID document;
- date of expiry of personal ID document.

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 IDENTIFICATION MEANS**

The electronic identification means according to the electronic identification via web interface 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 a document (file) containing persona identification data of the person, including graphic elements, such as a copy of the ID document, image of the signature, picture, etc.

The electronic identification means is generated at the request of the end user in real time. The electronic identification means is provided automatically to the relying party for certification of an online service. The relying party can trust the identity data of the person, in accordance with Regulation (EU) No. 910/2014.

The protection against attacks is carried out through complete measures, including DDOS defence systems, firewalls, reservation systems.

#### **4.3.1. ISSUANCE, PROVISION AND ACTIVATION**

The electronic identification means is issued by Evrotrust and is provided to the relying party through an API channel. During the entire process the session is encrypted by cryptographic keys.

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 relying party receives a document in text format through a specially developed data exchange interface. For data exchange between web applications and web services, Evrotrust uses one of the most popular data exchange formats - JSON file format to present the authenticated personal and other data of users in a structured text human-readable format.

#### **4.3.2. TEMPORARY SUSPENSION OF THE VALIDITY, REVOCATION AND REACTIVATION**

Due to the one-time nature of the identification, suspension, revocation and reactivation of the electronic identification means are not supported as policies.

For the purposes of re-activating an electronic identification means through a web interface process, the individual needs to go through consent and a new identification process again.

#### **4.3.3. RENEWAL AND REPLACEMENT**

Insofar as the identification is one-time and a new identification process is initiated if necessary, the renewal and replacement of the means of identification is not carried out as a process.

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

The electronic identification scheme represents an 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.

Due to the fact that the electronic identification is a one-time process, a policy of suspension or cancellation of the means of identification does not apply.

A request to terminate or revoke the entire identification scheme can be received from the Communications Regulation Commission or a state organization with powers in line with the national legislation.

#### **4.5. REQUIREMENTS RELATED TO THE INTEROPERABILITY**

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 assurance level "high" or "significant" depending on the specific implementation 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. 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 the electronic identification means is in line with the requirements of the standard ETSI TS 119 461. 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 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 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 a qualified electronic seal. 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 archive is signed by a qualified electronic seal.

*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.

### **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;
- 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 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 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 is to control the electronic identification activities, inasmuch as these activities are compatible with the implemented integrated management

system which includes the requirements of the ISO/IEC 27001<sup>1</sup>, ISO 9001<sup>2</sup>, ISO 22301<sup>3</sup>, and ISO/IEC 20000-1<sup>4</sup> standards, and of Regulation (EU) No 910/2014, Regulation (EU) 2016/679<sup>5</sup>, 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**

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 electronic identification services 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 its 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

---

<sup>1</sup> ISO 27001 Information technology. Security techniques. Information security management systems

<sup>2</sup> ISO 9001 Quality management systems

<sup>3</sup> ISO 22301 Societal security. Business continuity management systems

<sup>4</sup> ISO 20000-1 IT service management system

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 providers 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 and are caused by negligence or intentionally within a defined limit. 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. INVIOABILITY 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 software elements and databases related to the provided services 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;
- complying with the established operating procedures and rules for technical and physical control, in accordance with the terms of this document;
- issuing formalized documents with structured content containing users' personal data, 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;
- performing procedures for identification and verification of authenticity/identity of natural/legal persons;
- using reliable systems;
- taking immediate measures in case of occurrence of technical issues related to security;
- informing users and relying parties of their obligations and due diligence while using the electronic identification service provided by Evrotrust, and of the proper and safe use of the issued 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 via web interface and issuing of qualified certificates after such identification, in accordance with the national and European legislation;

- 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;
- 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;
- Evrotrust identifies users and provides electronic identification means remotely in line with ETSI TS 119 461 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 an internal procedure for the submission, review and 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 recommended software, such as browsers and settings, hardware for users, also forms, templates, General Terms and Conditions, 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 services;
- from omissions in establishing the person's identity due to negligence and non-compliance with the policies and practices defined in this document.

## 17.OBLIGATIONS OF USERS

The users of the identity verification service which includes the issuance of electronic identification means have the following obligations:

- to familiarize themselves and to comply with the terms and conditions of the General Terms and Conditions, 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 General Terms and Conditions, 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 accept the terms and conditions set out in the General Terms and Conditions of the contract between them 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 contents of which are the General Terms and Conditions. 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, including declaring of untrue personal data, 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 electronic identification means 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 AD

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

1766 Sofia, Bulgaria

telephone, fax: + 359 2 448 58 58

e-mail: [office@evrotrust.com](mailto:office@evrotrust.com)

➤ to Evrotrust's e-mail address ([office@evrotrust.com](mailto:office@evrotrust.com) or [dpo@evrotrust.com](mailto: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.*