POLICY AND PRACTICE

FOR PROVIDING A QUALIFIED SERVICE FOR ISSUING ATTRIBUTE CERTIFICATE

CONTENTS

1. INTRODUCTION

Evrotrust Technologies AD (Evrotrust) is a qualified trust service provider, carrying out its activity in accordance with the requirements of Regulation (EU) No 910/2014 and the Electronic Document and Electronic Trust Services Act; as such, it is entered in the trusted list of the European trust service providers (https://webgate.ec.europa.eu/tl-browser/#/tl/BG/6).

"Policy and Practice for Providing a qualified Service for Issuing Attribute Certificate" (the Policy/CP-CPS-ACA Policy and Practice for providing a qualified service for issuing attribute certificate) is a document describing the general rules, scope of application and procedures applied by Evrotrust when issuing qualified attribute certificates on the basis of identification with additional specific attributes for natural and legal persons.

The "Policy for Issuing Qualified Attribute Certificate" forms an inseparable part of the General Terms and Conditions of the Contract for Provided Trust, Information, Cryptographic and Consulting Services. Access to this service is available for Bulgarians as well as for foreign citizens.

1.1. OVERVIEW

The Policy for providing qualified attribute certificate describes the process whereby any natural person or a natural person representing a legal entity (managers, board members, authorized agents, etc., having representative power by operation of law) who is a user of Evrotrust, requests the issuance of a qualified attribute certificate for a qualified electronic signature. The certificate is issued to that person so that they can use a qualified electronic signature to sign an electronic document containing personal identification data (statement for providing personal data) within the scope necessary for their relations with a relying party (such as a bank, insurance company, etc.). The person assigns Evrotrust to include additional data of theirs in the qualified attribute certificate.

The qualified attribute certificate for a qualified electronic signature is issued upon conditions identical with those for the standard qualified certificate for electronic signature, but the type and scope of the data verified by it are different. The additional specific attributes are without prejudice on the interoperability and recognition of the qualified electronic signatures, inasmuch as the entered data comply with the applicable standards. The applicability of the qualified attribute certificate is connected with the persons' identification before relying parties.

The legal value of the qualified attribute certificate as a qualified certificate for qualified electronic signature is acknowledged everywhere in the European Union.

The possibility for personal data verification by Evrotrust through the issuance of qualified attribute certificates for qualified electronic signatures is regulated by Preamble (54) in conjunction with Art. 24 (1) and Art. 28, item. 3 of Regulation (EU) No 910/2014. The persons who request issuance of a qualified attribute certificate are users of the services of Evrotrust. They are identified and already have registration as Evrotrust users; however, for the purposes of the issued qualified attribute certificates, Evrotrust issues a new certificate, entering already confirmed personal data.

1.2. COMPLIANCE

Evrotrust provides a qualified service of issuing qualified attribute certificates, covering the requirements of item 5.5.1.3 (c) 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/ACA.

The qualified attribute certificates issued by Evrotrust comply with the requirements of Preamble (54) in conjunction with Art. 24 (1) and Art. 28, item 3 of Regulation (EU) No 910/2014 of Regulation (EU) No 910/2014. Taking into account cross-border interoperability of the formats of qualified electronic signatures and seals introduced by Regulation (EU) No 910/2014, the qualified atrribute certificates are without prejudice to the mandatory requirements set out in Regulation (EU) No 910/2014 and Regulation (EU) 2015/1501 regarding the requirements for the minimum set of person identification data uniquely representing any natural or legal person. On a national level, specific attributes are included in the qualified attribute certificates, such as national identification number (EGN), as well as other data requested by a user or a client; however, Evrotrust guarantees that they do not impede neither cross-border interoperability, nor recognition of the qualified attribute certificates and qualified electronic signatures/seals in the European Union.

The Policy complies with the following documents:

➢ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Regulation (EU) No 910/2014), and with the applicable laws in the Republic of Bulgaria;

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protecion Regulation);
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 General requirements;
- 319 412-2 Certificate profile for certificates issued to natural persons;
- 319 412-3 Certificate profile for certificates issued to legal persons.

1.3. POLICY NAME AND IDENTIFIER

The name of this document is: "Certificate Policy and Practice for Providing a Qualified Service for Issuing Attribute Certificate", and its identifier (OID) is: 1.3.6.1.4.1.47272.2.16.17.2.

The qualified attribute certificates issued for users by Evrotrust contain a policy identifier, which may be used by the relying parties when determining the applicability of certificates to a particular application, as described in Recommendation IETF RFC 3647.

2. PARTICIPANTS IN THE INFRASTRUCTURE

2.1. CERTIFYING AUTHORITY *EVROTRUST RSA OPERATIONAL CA*

Evrotrust RSA Operational CA issues qualified attribute certificates for users in accordance with this document and with the "Practice and Policy for Providing Qualified Trust Services". Evrotrust RSA Operational CA performs the following specific obligations:

- It accepts an electronic request for issuing qualified attribute certificates;
- It issues a qualified attribute certificate;
- It publishes and maintains issued qualified attribute certificates in accordance with the procedures described in the "Policies and Practices" of Evrotrust;
- It keeps the records (logs) of the qualified attribute certificates issuing process.

2.2. USERS

Any natural person, or any natural person representing a legal entity which has a contract with Evrotrust for a trust service of issuing an attribute certificate, is a user of this service provided by Evrotrust.

The provided trust service is also available for disabled persons, wherever that is practically possible.

2.3. RELYING PARTIES

A relying party to the provided service (this is Evrotrust's integrated partner) is defined as a natural or legal person who relies on a qualified electronic signature accompanied by a qualified attribute certificate. Relying parties should have basic knowledge and skills concerning the use of a qualified attribute certificate and they should rely on the circumstances certified by it 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 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 qualified attribute certificates are issued.

2.4. 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 certification service provision activities. Evrotrust uses subcontractors and service providers, such as specialized data centers, for reliable and secure colocation of server and network equipment, providers of cloud systems and services, providers of automated identification services, IT services and others. When working with subcontractors and providers, Evrotrust requires them to strictly follow its procedures, in accordance with this Policy and Practice.

3. USE AND APPLICABILITY OF AN ATTRIBUTE CERTIFICATE

3.1. APPLICABILITY OF AN ATTRIBUTE CERTIFICATE

The use and applicability of the qualified attribute certificate are related to signing statements for personal and/or other data provision, by natural persons, or by representatives of legal persons, upon their request, as needed for their relations with a third relying party. Users make a one-time use of qualified attribute certificates to sign a statement for personal and/or other data provision; in this way, they identify themselves and agree to the provision of personal and/or other data. Once registered, such persons may use their registration and may request for a qualified atrribute certificate to be issued electronically without limitation to the number of times; however, each validation shall require the use of a newly generated one-time pair of a private and a public key, accompanied by a new qualified atrribute certificate. The validity period of the qualified attribute certificate and its related public key is 2 (two) hours.

3.2. USE OF A QUALIFIED ATTRIBUTE CERTIFICATE BY RELYING PARTIES

Relying parties shall rely on the data from the qualified attribute certificate only after verifying the status of such data and the electronic signature of the certifying authority that has issued the certificate.

3.3. PROHIBITION ON THE USE OF AN ATTRIBUTE CERTIFICATE

Attribute certificates shall not be used in a way which is incompatible with their stated purpose and scope of applicability.

4. POLICY MANAGEMENT

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 version shall be developed by authorized competent employees of Evrotrust and it gets published following an approval by the Board of Directors. Users and relying parties 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 of Evrotrust Technologies AD – "Certificate Policy and Practice for Providing a Qualified Service for Issuing Attribute Certificate"

- is the CEO of Evrotrust.

Additional information may be received at the following address:

Evrotrust Technologies AD
Sofia, 1766
Business center MM, floor 5, Bul. Okolovrasten pat 251G
phone, fax: + 359 2 448 58 58
e-mail: office@evrotrust.com

5. DEFINITIONS

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

6. PUBLIC REGISTER

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

7. OPERATING ACTIVITIES FOR THE PURPOSES OF ISSUING AN ATTRIBUTE CERTIFICATE

Evrotrust verifies the identity of a person - the natural person to whom the signature belongs, or a representative of the legal person - through physical presence, or by using a system for remote identification of natural and legal persons in accordance with Art. 24, par. 1, letter "d" of Regulation (EU) 910/2014, in order to provide the serivce of issuing a qualified attribute certificate for qualified electronic signature to that person. Evrotrust guarantees that the information contained in the attribute certificates is true and correct at the time of their issuance.

The request for remote identification of a person is entered in the systems of Evrotrust by a relying party (such as a bank, an insurance company, etc.) through a specially developed communication interface. For the purposes of the identification, the natural person assigns Evrotrust to issue an attribute certificate electronically, with the necessary amount of data requested by the relying party.

In the event that the person is not an Evrotrust user, they must go through an identification process with Evrotrust and become an Evrotrust user, in accordance with the applied "Policies and Practices". The attribute certificate is issued by Evrotrust once, has short validity period, and contains verified public key and data beyond the mandatory attributes for a qualified certificate resulting from Regulation (EU) No 910/2014, in accordance with the applicability of the certificates and the relations of the client with the relying party. Evrotrust consults the primary registers for any changes that may have occured in the civil or professional status, in an ID document validity period, etc. Personal and other types of data are processed in a way that guarantees high level of security, including protection against unauthorized or illegal processing, against accidental loss, destruction, or damage, by applying appropriate technical and organizational measures ('entirety and confidentiality').

7.1. THE PROCESS OF ISSUING AN ATTRIBUTE CERTIFICATE

Issuing an attribute certificate for identification of a natural person or of a natural person representing a legal entity before a relying party through the Evrotrust mobile application or by physical presence before an Evrotrust representative includes going through the following steps:

➢ The relying party sends Evrotrust a request for identification of the person through a specialized web portal, API interface, or through an SDK module;

➢ Evrotrust checks whether that person is already an Evrotrust user, identified in accordance with the applicable "Policies and Practices" for trust services provision. In case the person is not yet a user, they are expected to identify themselves and conclude a contract with Evrotrust;

➢ In case the person is already identified by Evrotrust, the identification request by the relying party is sent to that person's mobile application, together with the required amount of data. In case the identification of the user is made by physical presence, the user is provided with the amount of data expected for the purposes of the identification before the relying party;

- ➢ The person requests Evrotrust to issue an attribute certificate for a qualified electronic signature, containing their personal and/or other data;
- ➢ The person confirms the issuance of an attribute certificate, thus assigning Evrotrust to generate a pair of a private and a public key, and to issue a qualified attribute certificate for the public key;
- ➢ Evrotrust performs an automated verification of the personal data of that person, checking them against the data from the person's registration as a user, and where integration is existant - against the data from the primary registers or from reliable data sources;
- ➢ Evrotrust generates the pair of cryptographic keys and issues the attribute qualified certificate for the public key from that pair;
- ➢ Evrotrust makes it possible for that person (by sending to their mobile device an SMS with a link or a PIN code for confirmation) to sign the statement for personal and/or other data provision using the attribute certificate.

7.2. ISSUING A NEW QUALIFIED ATTRIBUTE CERTIFICATE AND GENERATING A NEW PRIVATE KEY

For the cases when an already registered user wishes to use the electronic identification service again, before a new or before the same relying party, Evrotrust issues them with a new qualified attribute certificate and generates a new private key. Each qualified attribute certificate is valid for 2 (two) hours and can be used only once.

7.3. TERMINATING THE CONTRACT WITH EVROTRUST

The contract for providing a qualified service accessible through the Evrotrust application and concerning the issuance of an attribute certificate shall be terminated upon cancellation of a user account, in the event of a non-existant account in the mobile application, or upon expiry of the validity period of the certificate.

7.4. IDENTIFICATION AND VERIFICATION OF IDENTITY AFTER CANCELLING AN ACCOUNT

Where a functionality is activated through the mobile application of Evrotrust for deleting an account, and where in time a person wishes to have the service for issuing an attribute certificate provided, such person must pass through a new process of registration and identification. A new attribute certificate can also be issued after making second physical identification.

8. PHYSICAL SECURITY CONTROL

The measures taken in regard to the physical protection of the information data, of the technological systems, the premises and the supporting systems related to them, are described in the document "Practice for Providing Qualified Trust Services".

8.1. PREMISES AND PREMISES STRUCTURE

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

8.2. PHYSICAL ACCESS

The physical security of the systems for issuing and managing attribute certificates complies to the requirements of international standards and recommendations.

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

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

The physical security of the systems is described in the document "Practice for Providing

Qualified Trust Services".

8.3. 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 siginificant 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 a qualified service of issuing an attribute certificate. The database is kept on a differential basis: database, file systems and archives.

8.4. WASTE DISPOSAL

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

9. ORGANIZATIONAL CONTROL

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

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

9.1. CONTROL AND TRAINING REQUIREMENTS FOR EVROTRUST EMPLOYEES

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

10. EVENT RECORDINGS AND MAINTENANCE OF JOURNALS

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

Information about the electronic journals is generated automatically.

Journals with records of regstered 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.

11. VULNERABILITY AND ASSESSMENT

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

12. ARCHIVING

Evrotrust records and stores the information concerning the process of issuing and managing qualified attribute certificates for qualified electronic signature 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. Data are stored for a period consistent with the requirements of the internal and independent audits which are performed, as well as for the purposes of security breach investigations. Unless otherwise required, after using them for their intended purposes, the collected data are destroyed in a secure way.

13. 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.

14. TRANSFER OF ACTIVITY TO ANOTHER QUALIFIED TRUST SERVICE PROVIDER

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

- ➢ notifies the Supervisory Authority for its intention not later that 2 (two) months before the date of termination and transfer of activity;
- ➢ makes any effort and care to continute 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 accepting provider, together with all archives and all issued certificates;
- ➢ performs all the necessary activities for transferring the obligations for information maintenance to the receiving provider;

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

15. WITHDRAWAL OF THE QUALIFIED STATUS OF EVROTRUST

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

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

16. MANAGEMENT AND CONTROL OF TECHNICAL SECURITY

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

Services”.

16.1. GENERATION OF A KEY PAIR TO A CERTIFYING AUTHORITY

The provider generates pairs of cryptographic (RSA) keys to the basic and to the operating certifying authorities using a hardware cryptosystem (HSM/Hardware Security Module) with security level at FIPS 140-2 Level 3 or higher, or respectively CC EAL 4+ or higher.

The procedure is described in the document “Practice for Providing Qualified Trust Services”.

16.2. GENERATION OF A KEY PAIR TO AN USER

The cryptographic key pair (private and public) of the issued qualified attribute certificates for qualified electronic signature is generated by Evrotrust through the Evrotrust mobile application. For the generation of a key pair, a hardware security profile (HSM) is used, in accordance with Regulation (EU) No 910/2014.

16.3. KEY LENGTH

The length of the basic Evrotrust key "Evrotrust RSA Root CA“ is 4096 bits, with a combination of asymmetric and hashing algorithms: sha384-with-RSA.

The length of the key pair of the operating certifying authority "Evrotrust RSA Operational CA“ is 2048 bits, with a combination of asymmetric and hashing algorithms: sha256-with-RSA.

The length of the key pair of the operating authorities "Evrotrust TSA", "Evrotrust RSA QS Validation" and "Evrotrust RSA Validation“ is 2048 bits, with a combination of asymmetric and hashing algorithms: sha256-with-RSA.

The length of the key pair for qualified electronic signature of a user, generated through the infrastructure of Evrotrust, is 2048, 3072 or 4096 bits, with a combination of asymmetric and hashing algorithms: sha256-with-RSA.

16.4. CRYPTOGRAPHIC ALGORITHMS

All of the used algorithms comply with the technical specification ETSI TS 119 312. Evrotrust regularly monitors the security and applicability of the hashing algorithm which is used.

All of the used algorithms go through an annual check, or are checked upon the occurrence of any changes. If the algorithm is compromised or has become unsuitable, a regeneration of all affected keys is initiated.

For every maintained account, Evrotrust monitors the strength of each cryptographic algorithm used with regard to the respective account. If any of the used algorithms or parameters is considered less secure, or if the validity of the respective certificate is about to expire, such algorithm or parameter is updated, or a new account is created.

16.5. PRIVATE KEY PROTECTION AND CONTROL OF THE CRYPTOGRAPHIC MODULE

The private keys of the certifying authorities of Evrotrust as well as the users' keys are stored in a secure cryptographic module which complies to the requirements of Regulation (EU) No 910/2014. The cryptosystem (Hardware Security Module/HSM) has a high level of security, being certified for security level FIPS 140-2 Level 3.

The private keys of the certifying authorities of Evrotrust are accessible via access codes divided into several parts - known to authorized persons from the Evrotrust staff. The basic certifying authority of Evrotrust is in an Offline mode. Along with the generation of the certifying authority's key pair, the procedure for storing the private key (or key pair) in accordance with an established internal procedure is also performed. For managing the private keys of Evrotrust which are stored in the cryptomodule, two out of four sets with the three roles of operator tokens and the corresponding personal identification numbers (PIN) for access are necessary. Initial key archive is made after the creation of all keys, and subsequently - after regeneration of some of them. The archiving of private keys stored in the cryptosystem (HSM) with security level FIPS 140-2 Level 3 is performed on a device with the same security level. To archive the keys, two of the four persons having tokens for access to the cryptosystem (HSM) are needed. Archiving is performed in a secure environment. After the archive (Backup) is created, it is put in a safe at a remote location, with the necessary security measures.

The private key of the user is generated and stored in an ecrypted version in the hardware cryptomodule which complies to the requirements of Regulation (EU) 910/2014 as Qualified Electronic Signature Creation Device (QSigCD); it is accessible via a personal access code. Private keys are destroyed by deleting the key or the respective slot.

17. COMPUTER SYSTEMS SECURITY

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

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

17.1. TECHNOLOGY SYSTEM LIFECYCLE SECURITY

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

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

17.2. NETWORK SECURITY

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

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

18. VERIFICATION AND CONTROL OVER THE ACTIVITY OF EVROTRUST

18.1. INTERNAL AUDITS

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

18.2. 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 Evrotrust and the trust services provided by it meet the requirements set out in Regulation (EU) No 910/2014.

Evrotrust is subject of audit at least once every 36 month by an independent verification team concerning the international standards ISO/IEC 27001, ISO 9001, ISO 22301, ISO/IEC 20000-1. The purpose of the audit is to confirm that the activity complies with the implemented integrated management system.

18.3. AUDIT BY THE NATIONAL SUPERVISORY BODY

The National Supervisory Body may, at any time, carry out an audit, or request that the Conformity Assessment Body perform an assessment for the conformity of Evrotrust's activity with the requirements of Regulation (EU) No 910/2014.

19. FINANCIAL RESPONSIBILITIES

Evrotrust is responsible for the service provided to the users and the relying parties who rely on the attribute certificates. Evrotrust is liable if damages are due to its fault, or to the fault of the parties to whom it has assigned the issuance of attribute certificates. If Evrotrust acknowledges and agrees that damages have occurred, it undertakes to pay such damages which are a direct and immediate consequence of the negligence of its employees. The maximum payment limit may not exceed the amount of the damages and may not be more than the limit set in the issued attribute certificate.

20. INSURANCE OF ACTIVITY

Evrotrust takes out a compulsory insurance of its activity, which shall also include its activities on providing the service of issuance of an attribute certificate. Evrotrust is liable for intentional damages, or damages that have occurred due to the negligence of a natural or a legal person because of the internal RA's failure to fulfil its obligations. The external RA, to whom Evrotrust assigns activities for provision of specific trust services, shall be liable for intentional damages, or damages which have occurred due to the negligence of a natural person or a legal entity because of the RA agents' failure to fulfil their obligations.

21. 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 of the requirements for confidentiality and non-distribution of personal data of persons that became known while issuing attribute certificates by the RA operators.

22. INTELLECTUAL PROPERTY RIGHTS

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

23. LIABILITIES, RESPONSIBILITY AND GUARANTEES OF EVROTRUST

23.1. GUARANTEES AND LIABILITIES

Evrotrust guarantees that it carries out its activity by:

➢ strictly complying to the conditions of this document, the requirements of Regulation (EU) No 910/2014, Regulation (EU) 2016/679, and the national legislation in the performance of its activity as a Qualified Trust Service Provider;

➢ ensuring that the provided service does not infringe copyrights and licensed rights of third parties;

➢ using technical equipment and technologies which ensure reliability of the systems and of the technical and cryptographic security during process implementation, including also a safe and secure mechanism/device for generating keys and creating an electronic signature in its infrastructure;

- issuing qualified attribute certificates for qualified 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;
- ensuring that there are conditions for precise verification of the time of issuance and termination of the certificates;
- ensuring measures against forgery of qualified attribute certificates and confidentiality of the data to which it has access during the process of creating the signature;
- using reliable systems for storing and managing the certificates;
- taking immediate measures in case of occurrence of technical issues related to security;
- upon expiration of the validity of the certificate, revoking its validity;
- informing users and relying parties on their obligations and due diligence while using or relying on the trust services provided by Evrotrust, and on the proper and safe use of the issued attribute certificates and the provided electronic identification related to them;
- using and storing the collected personal and other type of information solely for the purposes of its activity for providing electronic identification in accordance with the national legislation;
- not storing and not copying data for creating user's private keys;
- keeping available such means as to make its activity possible;
- concluding an insurance for the time of its activity;
- keeping trusted staff with the necessary expert knowledge, experience and qualification for carrying out the activity;
- maintaining Public Register/Storage;

- providing constant access to the Public Register electronically (24/7/365);
- ensuring protection against changes added to the Public Register kept by it, by means of unauthorized and unlawful access, or due to unforeseeable circumstances;
- providing conditions for each relying party to verify the status of an issued and published attribute certificate in the Public Register of certificates;
- performing periodic internal and external audits of its activity;
- using certified software and hardware as well as secure and reliable technological systems for its activity;
- maintaining, on the website of Evrotrust, a list of registration authorities, a list of recommended software and hardware for users, forms, templates, a standard contract, and other documents for the benefit of users;

23.2. RESPONSIBILITIES

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

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

24. OBLIGATIONS OF USERS

The users (natural persons and representatives of legal persons) of the attribute certificate provision service have the following obligations:

- to familiarize themselves and to comply with the terms and conditions of the Contract, of the Policies and Practices for trust service provision by Evrotrust, as well as with the requirements of other documents on attribute certificate issuance published in the Evrotrust Public Register;
- upon submitting requests for issuance of qualified attribute certificates, to provide true, correct and complete information, as required by Evrotrust in accordance with the Contract, with the legal requirements, with the applicable Policies and Practices;
- in case of any discrepancy between the provided information and the confirmed content, the user must immediately inform Evrotrust;
- to confirm the terms and conditions set out in the Contract between the user and Evrotrust;
- not to disclose their PIN code for access to their data in the mobile application, nor to provide third parties with their biometric features (fingerprint, face casts, etc.)

25. RESPONSIBILITY OF THE USER

The user's responsiblity 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 a service of attribute certificate issuance with registered legal person, such person shall be responsible for the damages.

26. DISCLAIMER

Evrotrust shall not be responsible in case of damages caused by illegal actions of users or relying parties, or by unforeseeable circumstances characterized as force majeure, including malicious actions of third parties (hacker's attacks, etc.)

27. PROFILE OF QUALIFIED NATURAL PERSON ATTRIBUTE CERTIFICATE FOR QUALIFIED ELECTRONIC SIGNATURE "EVROTRUST QUALIFIED NATURAL PERSON ATTRIBUTE CERTIFICATE FOR QES“

Evrotrust issues qualified attribute certificates using the same account for natural persons and for natural persons representing legal entities. For the different users, there is only variation in the data verified as part of the certificate profile.

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Operational CA
	OU=	Qualified Operational CA
	O=	Evrotrust Technologies JSC
	organizationIdentifier (2.5.4.97)= (2.5.4.97)	NTRBG-203397356
	C=	BG
Valid from	[starting date and time by UTC of the certificate validity]	
Validit to	[ending date and time by UTC of the certificate validity]	
Subject	C= (countryName)	Country: Two - letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Common name: Full name of the physical person in Latin by identity document
	G= (givenName)	Given name: Name of the physical person in Latin by identity document
	S= (surname)	Surname: Surname of the physical person in Latin by identity document
	name*= (id-at-name)	Full name: Full name of the physical person in Cyrillic by identity document.
	SERIALNUMBER= (serialNumber)	National identifier of the physical person in conformity to ETSI EN 319 412-1 т.5.1.3, for example: PNOBG-8310257645 for Civil Identification Number or another identifier which is associated with the physical person.

<table>
<tr><td></td><td>gender*=
(id-pda-gender)</td><td>Gender of the physical person at birth: M or F (male/female)</td></tr>
<tr><td></td><td>dateOfBirth*=
(id-pda-dateOfBirth)</td><td>Birth date with accuracy to days in ZULU format, for example: 19831231120000Z</td></tr>
<tr><td></td><td>description*=
(id-at-description)</td><td>Date from the machine-readable sections of the physical person identity document (Machine-readable passport)
<table>
<tr><th>Position</th><th>Length</th><th>Symbol</th><th>Meaning</th></tr>
<tr><td>1</td><td>1</td><td>alpha</td><td>I, A or C</td></tr>
<tr><td>2</td><td>1</td><td>alpha &lt;</td><td>Type: It is filled in at the discretion of the issuing country or authority. IP for passport and ID for national identity card are most often used.</td></tr>
<tr><td>3-5</td><td>3</td><td>alpha &lt;</td><td>Code of the country, issuing the identity document in conformity to (ISO 3166-1 alpha-3 code with modifications)</td></tr>
<tr><td>6–14</td><td>9</td><td>alpha num &lt;</td><td>Number of identity document</td></tr>
<tr><td>15</td><td>1</td><td>num &lt;</td><td>Control number of the digits 6–14</td></tr>
<tr><td>16</td><td>1</td><td>:</td><td>Divider</td></tr>
<tr><td>17</td><td>6</td><td>num</td><td>Year, month and date (YYMMDD) to which the identity document is valid</td></tr>
<tr><td>18</td><td>1</td><td>:</td><td>Divider</td></tr>
<tr><td>19</td><td>6</td><td>num</td><td>Year, month and date (YYMMDD) when the identity document is issued</td></tr>
</table>
For example:
<b>ID</b>BGR<b>641020223</b>4<b>:</b>201013:251013</td></tr>
<tr><td>Public Key Type/Length</td><td colspan="2">RSA (2048 / 3072/ 4096 Bits)</td></tr>
<tr><td>Subject Key I</td><td colspan="2">[Calculated value for the issued certificate]</td></tr>
</table>

<table>
<tr><td>Authority Key Identifier</td><td>Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08</td></tr>
<tr><td>CRL Distribution Points</td><td>[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl</td></tr>
<tr><td>Authority Information Access</td><td>[1]Authority Info Access
Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
Alternative Name:
URL=http://ca.evrotrust.com/aia/EvrotrustRSAOperationalCA.crt
[2]Authority Info Access
Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name:
URL=http://ca.evrotrust.com/ocsp</td></tr>
<tr><td>Enhanced Key Usage</td><td>Client Authentication (1.3.6.1.5.5.7.3.2)
Secure Email (1.3.6.1.5.5.7.3.4)</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.2.1
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps
[2]Certificate Policy:
Policy Identifier=0.4.0.194112.1.2</td></tr>
<tr><td>Key Usage (critical)</td><td>Non-repudiation (Bit 1), Digital Signature (Bit 0), Key Encipherment (Bit 2)</td></tr>
<tr><td>QCStatements</td><td>
<table>
<tr><td>id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)</td><td>id-etsi-qcs-semanticsId-<b>Natural</b> (oid=0.4.0.194121.1.1)</td></tr>
<tr><td colspan="2">id-etsi-qcs-<b>QcCompliance</b> (oid=0.4.0.1862.1.1)</td></tr>
<tr><td>id-etsi-qcs-<b>QcLimitValue</b>[ii] (0.4.0.1862.1.2)</td><td>[Amount in BGN or EUR]</td></tr>
<tr><td colspan="2">id-etsi-qcs-<b>QcSSCD</b> (oid=0.4.0.1862.1.4)</td></tr>
<tr><td>id-etsi-qcs-<b>QcType</b> (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-<b>esign</b> (oid=0.4.0.1862.1.6.1)</td></tr>
<tr><td>id-etsi-qcs-<b>QcPDS</b> (oid=0.4.0.1862.1.5)</td><td>PdsLocations
PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf
language=en</td></tr>
</table>
</td></tr>
</table>

**The fields marked with asterisk may not be present in the certificate*

28. DISPUTE RESOLUTION

Only dissimilarities or contradictions between persons who are parties to the contract with Evrotrust may be subject to disputes. Disputes or complaints regarding the issuance of attribute certificates provided by Evrotrust will be solved by intermediation, on the basis of information submitted in a written form. Claims shall be submitted in a written form, to the address of Evrotrust.

29. 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.