CERTIFICATE POLICY

FOR QUALIFIED CERTIFICATION SERVICES FOR WEBSITE AUTHENTICATION

Version: 1.1

	Position	Name, surname	Date	Signature
Approved by	Executive Director	Konstantin Bezuhanov	*23.06.2017*	
Agreed by	Representative of the management for ISMS	Stefan Hadzhistoychev	*23.06.2017*	
Developed by	Consultant for ISMS	Mariya Vladimirova	*23.06.2017*	

Date of the document registration:	*23.06.2017*
The original is stored:	*at Representative of ISMS management*

Type of the copy and serial number

Original	X	**Controlled copy**		**Informational**	

Distribution of the document:	**Subscriber:**
Internal:	
External:	

This document is part of the Information Security Management System of EVROTRUST TECHNOLOGIES INC.
Everyone who uses this document shall carry out the ISMS requirements for work with sensitive information.

CONTENTS

1 INTRODUCTION

"Certificate Policy for Qualified Certification Services for Website Authentication" (Policy/CP) is a document that describes the general rules and norms applied by “EVROTRUST TECHNOLOGIES” AD (EVROTRUST/EVROTRUST) when creating, verifying and validating Qualified Certificates for Website Authentication and their scope of applicability.

The website authentication trust services offered by EVROTRUST provide a means by which every visitor can be sure that behind the website is a real and legitimate subject. EVROTRUST

The trust website authentication services offered by EVROTRUST are in accordance with 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), the requirements and guidelines of the CA/Browser Forum (https://cabforum.org/) and in accordance with the applicable legislation in the Republic of Bulgaria.

The Qualified Website Authentication Certificate profile is defined in this document based on the requirements of the CA/Browser Forum (Baseline requirements). This profile can be used for certificates for legal entities and natural persons.

For the issuance of a qualified website authentication certificate by EVROTRUST are applied procedures ensuring a high level of reliability and security of the authenticated information identifying the Users.

The relations between EVROTRUST and the User are governed by a contract for qualified trust services.

The prices of the website authentication certificates are contained in the document "Trust, Information, Cryptographic and Advisory Services Tariff" of EVROTRUST available on the EVROTRUST website.

1.1 REVIEW

The document "Certificate Policy for Qualified Certification Services for Website Authentication" refers to qualified certificates issued by EVROTRUST as defined in Regulation (EU) No 910/2014.

This document is structured in accordance with the framework defined in the IETF RFC 3647 Recommendation "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

The policy is a public document. It can be changed at any time by EVROTRUST, and any new

version is communicated to interested parties by publishing it on the Evrotrust website: https://www.evrotrust.com.

1.2 NAME AND IDENTIFICATION OF THE DOCUMENT

This document has the full title "Certificate Policy for Qualified Certification Services for Website Authentication" by “Evrotrust Technologies” AD.

As described in IETF RFC 3647 Recommendation, the certificates include a policy identifier that can be used by the Relying Parties to determine the reliability and validity of an application.

EV certificates pass a very rigorous verification procedure and require a longer release period. It is necessary to identify the legal entity that controls the website by name, seat, management address, incorporation or registration, and registration number or other data for the identification of the said entity, as well as to check for encrypted communication with the website. Additional checks are made to establish the business's legality and the impossibility of spreading malware or other online fraud.

The Domain Validation Certificate Policy (DVCP) identifier has the policy OID=1.3.6.1.4.1.47272.2.4.1 and corresponds to itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6), c OID=0.4.0.2042.1.6.

DV Certificates, with Extended Normalized Certificate Policy (NCP+) requiring a secure user device, are issued after confirmation by EVROTRUST that the use of the domain by the owner has been established. This is done by the Certification Authority, which sends an email request to the domain owner to fill in the database with the required information. Once the owner replies, the certificate is issued. The Certification Authority may carry out additional inspections to minimize frauds in issuing the certificate. The certificate only contains the domain name.

The Organizational Validation Certificate Policy (OVCP) identifier has the policy OID=1.3.6.1.4.1.47272.2.4.2 and corresponds to itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7), c OID=0.4.0.2042.1.7.

For OV Certificates, with Extended Normalized Certificate Policy (NCP+) that requires a secure user device, the Certification Authority should verify and confirm the company/legal entity name, domain name, and other information by using public databases. The Certification Authority may also use additional methods for information verification to verify the authentication of the information included in the certificate. The certificate issued must contain the name of the company and the name of the domain for which the certificate was issued. Due to these additional checks, this certificate is recommended to

be used in e-commerce transactions as it provides Users with additional business information.

This document identifies a policy identifier of qualified certificates for a **QCP-w** website. This policy offers a high level of security and reliability as defined in Regulation (EU) No 910/2014.

To each of the policies, under which qualified certificates of EVROTRUST are issued, shall be assigned an Object Identifier (OID).

The values of the object identifiers are:

Qualified service	Object Identifier (OID)
Evrotrust SSL Domain Validated Certificate	1.3.6.1.4.1.47272.2.4.1 (corresponds to a policy with OID = 0.4.0.2042.1.6)
Evrotrust SSL Organization Validated Certificate	1.3.6.1.4.1.47272.2.4.2 (corresponds to a policy with OID = 0.4.0.2042.1.7)

1.3 PARTICIPANTS IN THE EVROTRUST INFRASTRUCTURE

EVROTRUST as a Qualified Trust Service Provider provides generation and management services (suspension, renewal and termination) of Qualified Website Authentication Certificates through the “Evrotrust RSA Operational CA” Certification Authority and IDENTIFICATION AND IDENTITY ESTABLISHMENT services to users (natural persons and legal entities) through the Registration Authority. Other participants in the infrastructure of EVROTRUST are Users and Relying Parties.

1.3.1 CERTIFICATION AUTHORITIES

1.3.1.1 BASIC CERTIFICATION AUTHORITY ("EVROTRUST RSA ROOT CA")

"Evrotrust RSA Root CA" issues qualified electronic certificates that are hierarchically dependent in terms of the infrastructure in the EVROTRUST domain. The Basic Certificate of EVROTRUST is self-issued and self-signed with the basic private key of EVROTRUST. With the basic private key EVROTRUST signs certificates for public keys of its Operational Certification Authorities.

1.3.1.2 OPERATIONAL CERTIFICATION AUTHORITY ("EVROTRUST RSA OPERATIONAL CA")

"Evrotrust RSA Operational CA" is a certification authority that issues qualified website authentication certificates that are governed by this Policy.

1.3.2 REGISTRATION AUTHORITY

The Registration Authority is a separate structure of EVROTRUST, but it can also be an external legal entity, to which EVROTRUST assigns the services of registration, IDENTIFICATION AND IDENTITY ESTABLISHMENT of users of EVROTRUST.

Contact details of the Registration Authority of EVROTRUST are available on the EVROTRUST Website.

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

1.3.3 USERS

A user may be any natural person or legal entity who has a written contract with EVROTRUST for the issuance and management of a Qualified Website Authentication Certificate.

Where practicable, the trust services provided and the products used to provide these services are also available to disabled persons.

1.3.4 RELYING PARTIES

A Relying Party is a natural person or legal entity that relies on a qualified certificate of website authentication issued by the infrastructure of EVROTRUST.

1.3.5 OTHER PARTICIPANTS

1.3.5.1 VALIDATION AUTHORITIES

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

1.4 USE OF QUALIFIED CERTIFICATES

The applicability of a Qualified Website Authentication Certificate is determined primarily by the described values of the attributes contained in the certificate that are determined by EVROTRUST. Certificates may also contain additional restrictions set forth in this Policy.

1.4.1 RECOMMENDED APPLICATION SCOPE

Private keys belonging to a Qualified End User Website Authentication Certificate issued by

EVROTRUST and based on this Policy may only be used for Website Authentication.

1.4.2 BAN ON THE USE OF QUALIFIED CERTIFICATES

The use of qualified website authentication certificates issued by EVROTRUST in accordance with this Policy and the private keys belonging to these certificates are forbidden to be used for purposes other than website certification.

Qualified certificates issued in accordance with this Policy may not be used for unlawful purposes.

1.5 POLICY MANAGEMENT

1.5.1 ORGANIZATION MANAGING THE POLICY

EVROTRUST is responsible for the management of this Policy.

Each version of the Policy is in force until the approval and publication of a new version. Each new version is developed by EVROTRUST employees and after approval by the EVROTRUST Board of Directors it is published.

Users are required to comply only with the valid version of the Policy at the time of use of EVROTRUST services.

1.5.2 CONTACT PERSON

The contact person for the management of the document "Certificate Policy for Qualified Certification Services for Website Authentication" from EVROTRUST TECHNOLOGIES AD is the executive director of EVROTRUST.

Further information can be obtained at:

Evrotrust Technologies AD

Sofia, 101 “Tsarigradsko Shose” Blvd.

Business Centre “AKTIV”, 6th floor

Telephone, Fax: + 359 2 448 58 58

Email: office@evrotrust.com

1.5.3 PERSON OR ORGANIZATION RESPONSIBLE FOR THE CORRECTNESS OF THE POLICY AND PRACTICE

EVROTRUST, which issues the "Certificate Policy for Qualified Certification Services for Website Authentication", is responsible for its compliance with the "Certification Practice Statement for Qualified Trust Services" as well as for the provision of the Trust Service in accordance with the provisions contained in this document.

The Policy and Practice are published in the Public Register of EVROTRUST and are available to Users and Relying parties 24 hours a day, 7 days a week, 365 days a year at: https://www.evrotrust.com.

1.5.4 PROCEDURES FOR THE PRACTICE APPROVAL

"Certification Practice Statement for Qualified Trust Services" (CPS) includes the procedures for providing Qualified Website Authentication Certificates.

Each version of the "Certification Practice Statement for Qualified Trust Services" is in force (has a current status) until the approval and publication of a new version. Each new version is developed by EVROTRUST employees and, after approval by the Board of Directors of EVROTRUST, is published.

1.6 DEFINITIONS AND ABBREVIATIONS

1.6.1 DEFINITIONS

Subject - In the case of certifying the authentication of a website, it is a web server that is identified by a domain name or IP address;

Person identification data - means a set of data enabling the identity of a natural person or legal entity;

Qualified Trust Services Provider - means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

Qualified Website Authentication Certificate - means a website authentication certificate that is issued by a qualified trust service provider and meets the requirements of Regulation (EU) No 910/2014;

Trust service - means an electronic service normally provided for remuneration which consists of: the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or; the creation,

verification and validation of certificates for website authentication; or; the preservation of electronic signatures, seals or certificates related to those services;

Qualified Trust Service - means a trust service that meets the applicable requirements laid down in Regulation (EU) No 910/2014;

Relying Party – natural persons or legal entities, as well as persons from the state, public and political sectors that are addressees of electronic statements. The Relying Party relies on a trust service;

Policy Approval Authority/PAA – An authority authorized to approve, monitor, and maintain the Certification Policy;

Compliance Assessment Body - A body that is accredited in accordance with Regulation (EC) No 765/2008 as competent to assess the compliance of a qualified trust service provider and the qualified certification services provided by that provider;

Practice (CPS) - "Certification Practice Statement for Qualified Trust Services" is a document containing rules on the issuance, suspension, resumption and termination of certificates as well as the conditions for access to certificates;

CRL/Certificate Revocation List - The list contains certificates that can no longer be considered valid. The CRL is signed with the electronic signature of the Certification Authority;

Secure user device - a device that holds the User's private key, protects this key from compromising and signs or decrypts on behalf of the User;

Private Key - A string of symbols that is used in an algorithm to convert information from a readable into ciphered (encrypted) form or vice versa – from a ciphered into a readable form (decryption);

Public Key - One of a pair of keys used in an asymmetric cryptosystem that is accessible and can be used to verify an electronic signature/seal;

Public Register/Repository - A data repository containing all issued, suspended, terminated and renewed certificates. Certificates are available to Users and Relying parties.

1.6.2 ABBREVIATIONS

CA - Certification Authority;

CP (Certificate Policy) - Certificate Policy for Qualified Certification Services for Website Authentication;

CPS - Certification Practice Statement;

CRL - Certificate Revocation List;

HSM - Hardware Security Module;

Issuer;

LDAP - Lightweight Directory Access Protocol;

OID - Object Identifier;

PKI - Public Key Infrastructure - the combination of hardware, software, personnel, documentation in EVROTRUST for the creation, use, management and verification of issued electronic signature/seal certificates;

RA - **Registration Authority**;

SSL - Secure Socket Layer;

OCSP - **Online Certificate Status Protocol**;

TSP - **Trust Service Provider**.

2 RESPONSIBILITY FOR PUBLISHING AND THE REPOSITORY

2.1 REPOSITORY

The EVROTRUST public register is a repository of current and previous versions of electronic documents, including up-to-date versions of "Certificate Policy for Qualified Certification Services for Website Authentication" and "Certification Practice Statement for Qualified Trust Services" intended for Users, Certificates of Certification Authorities, User Certificates, Certificate Revocation Lists, and other information.

The repository is managed and controlled by EVROTRUST.

All users and relying parties have permanent access to all information in the repository at: https://www.evrotrust.com.

2.2 INFORMATION PUBLISHED BY EVROTRUST

The qualified certificates issued are stored in a database of EVROTRUST. Access to these certificates can be accomplished through an Online Certificate Status Protocol in real-time.

For online verification of data from the register it is necessary to use appropriate software (OCSP-client) or access through the provider's website.

Verification of issued qualified certificates can also be made on the CRL, which is published on the EVROTRUST web page and is updated every 3 (three) hours or more.

2.3 FREQUENCY OF PUBLICATION

The documentation, including the Policy and Certification Practice Statement for Qualified Trust Services, agreements, forms, electronic signature/seal operation manuals, audit reports, etc. issued by

EVROTRUST, is published on the EVROTRUST website immediately upon each update.

Operational certificates of the Certification Authority are published immediately upon each issue of new certificates.

An update of the Public Register with the issued user qualified certificates shall be made automatically and immediately after the publication of each newly issued valid certificate.

An update of the current CRL is automatically made no more than 3 (three) hours or immediately after the revocation or suspension/resumption of a valid certificate.

2.4 ACCESS TO PUBLICATIONS

EVROTRUST offers directory services for the information stored in the repository (public register), by providing HTTP/HTTPS and OCSP-based access.

The access to the information in the repository is not limited by EVROTRUST, except at the request of the User and only in respect to its validly issued qualified certificate.

The information published in the repository of EVROTRUST is permanently accessible (24/7/365), except in cases of events beyond EVROTRUST's control.

3 IDENTIFICATION AND IDENTITY ESTABLISHMENT

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

3.1 NAMES

The requirements for the data included in the end-user certificates issued are in accordance with this Policy.

The Issuer and Subject identifiers listed in the main fields of the certificate must comply with the RCF 5280 [20] and RFC 6818 [21] Recommendations and meet the requirements for specific name formats.

The name and other identifying marks of the natural person or legal entity in the relevant fields for each type of certificate are in accordance with the DN (Distinguished Name) formed according to the standard X.500 and X.520.

EVROTRUST may issue a qualified certificate using a "pseudonym" to name a natural person only after the Registration Authority has collected the necessary information about its identity and has successfully identified it.

The names included in the Distinguished Name (DN) of the user have their meaning in Bulgarian or in another foreign language.

3.1.1 NAME OF A WEB SERVER (SUBJECT)

This Policy requires the following fields related to the identification of the subject in the certificate:

- **Common Name (CN), OID: 2.5.4.3**

A domain name or IP address is optionally saved in the Website's Certificate of Authentication. The use by the User of the domain name or IP address is legal. The domain name or IP address can be saved in the specified field or in the Subject Alternative Names.

A pseudonym cannot be saved in the CN field. Fill in the box is required.

- **Surname, OID: 2.5.4.4**

In the field, the name of the natural person, who owns the website, is filled in. Fill in this box is optional.

- **Name (Given Name), OID: 2.5.4.42**

In the field, fill in the name/first name of the natural person who owns the website. Fill in this box is optional.

- **Pseudonym, OID: 2.5.4.65**

The Web Server Authentication Certificate cannot be issued under a pseudonym.

- **Serial Number, OID: 2.5.4.5**

If the field is used, it is required to specify an identifier in it. The use of a serial number is in accordance with RFC 4043 [19] Recommendation. EVROTRUST ensures that the serial number is unique in the EVROTRUST system. Fill in this box is optional.

- **Organization (O), OID: 2.5.4.10**

The Website Authentication Certificate may contain the full or abbreviated name of the organization. The use of this field is mandatory if the certificate is issued to an organization.

- **Organization Identifier, OID: 2.5.4.97**

The field is filled in, if the certificate is issued to an organization. If the certificate is issued to a

natural person, this field is not filled in. Fill in this box is optional.

- **Organizational Unit (OU), OID: 2.5.4.11**

The field may be filled in, if the certificate is issued to an organization. A trademark or other organizational unit information may be entered in the field. The information to be filled in this field is entered after it has been certified by EVROTRUST. If the certificate is issued to a natural person, these fields are not filled in. Fill in this box is optional.

- **Country (C), OID: 2.5.4.6**

When issuing an organization certificate, a two-letter code of the country, in which the organization is established, is filled in this field. If the name of the organization is not included in the certificate, but the domain name or IP address and the country cannot be identified, the alphabetic code of the country of the User, who has filed the certificate, is entered. Fill in this field is required.

Fill in this field is required. In the case of entering the code of Bulgaria, the value of the field is "BG".

- **Address (Street Address/SA), OID: 2.5.4.9;**

In the case of issuing an organization certificate, in the field is entered the address which is the place of establishment of the organization. The field is filled in after the information is verified and confirmed. Fill in this box is optional.

- **Locality Name (L), OID: 2.5.4.7;**

In the case of issuing an organization certificate, this field shall include the name of the settlement where the organization is established. Fill in this box is optional.

- **State or Province Name, OID: 2.5.4.8;**

In the case of issuing an organization certificate, this field shall include the name of the settlement where the organization is established. Fill in this box is optional.

- **Postal Code, OID: 2.5.4.17;**

In case of issuance of an organization certificate, in this field the postal code of the settlement, where the organization is established, is entered. Fill in this box is optional.

- **Title (T), OID: 2.5.4.12**

The field is not filled in.

- **E-mail address (EMAIL), OID: 1.2.840.113549.1.9.1**

E-mail address of the web server. The field is not filled in.

Certificates issued in accordance with this policy may additionally contain fields in “Subject DN”. They may contain only verified data.

3.1.2 ALTERNATIVE NAMES

The “Subject Alternative Names” field is not on the list of critical extensions in the certificate. The field must always contain at least one domain name or IP address. Fill in the box is required. This field can list all domains/IP addresses, even those in the "CN" field.

3.1.3 NECESSITY OF MEANINGFUL NAMES

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

3.1.4 ANONYMITY OR PSEUDONYMS OF USERS

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

3.1.5 RULES FOR INTERPRETATION OF DIFFERENT NAME FORMS

In order to correctly interpret the fields included in the EVROTRUST certificates, EVROTRUST recommends that the Relying Parties act as described in this document. The Relying Party, in case of necessity of interpreting an identifier or other data described in the certificate, can directly contact EVROTRUST on the phones listed on the company's website.

EVROTRUST may include in the User Qualified Certificates information on electronic identification of a natural person or legal entity that has been successfully verified and confirmed by the Registration Authority on the basis of the User's identity documents submitted. The information provided does not go beyond what is strictly necessary for User identification.

3.1.6 UNIQUENESS OF NAMES

The Subject (Web server/Subject) must have a unique name in the certificate register of EVROTRUST. To ensure uniqueness, EVROTRUST, if necessary, includes a unique identifier (OID) that is included in the “Subject DN Serial Number” field.

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

3.1.7 RECOGNITION, CERTIFICATION OF AUTHENTICATION AND ROLE OF THE TRADE MARK. DISPUTE SETTLEMENT PROCEDURE.

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

3.2 INITIAL REGISTRATION

EVROTRUST uses each communication channel within the limits provided by the law to verify the identity of the natural person or legal entity requesting the issuance of a certificate as well as to verify the authentication of the data provided.

EVROTRUST may refuse to issue a certificate at its sole discretion without justification.

3.2.1 VERIFICATION OF PRIVATE KEY POSSESSION

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

3.2.2 CERTIFICATION OF THE IDENTITY OF A LEGAL ENTITY

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

3.2.3 CERTIFICATION OF THE IDENTITY OF A NATURAL PERSON

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

3.2.4 SPECIAL ATTRIBUTES

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

3.2.5 UNCONFIRMED INFORMATION

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

3.2.6 CHECKING BY THE CERTIFICATION AUTHORITY

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

3.2.7 INTEROPERABILITY

EVROTRUST may cooperate with other Providers during the provision of Qualified Trust Services but only with those who agree to comply with the requirements of this Policy.

EVROTRUST needs to make sure that there is no legislative barrier to the cooperation on public service provision.

As a result of the cooperation, the rights of the clients must not be violated in any way and the quality of service should not be impaired.

3.2.8 DOMAIN NAME AUTHENTICATION

A website authentication certificate must contain at least one domain name or IP address.

Prior to the issuance of a website authentication certificate, EVROTRUST confirms the authentication of the domain name or IP address. In order for the name to be entered in the certificate, EVROTRUST checks the possibility for the subject to use the domain name or IP address. During the check, the confirmation should be obtained from authentic entries or from a trusted third party. Confirmation is obtained, if it is proven in practice that the subject has control over a given domain name or IP address. If more than one domain or IP address is specified in the certificate, the above check is performed on a case-by-case basis.

3.2.9 CRITERIA OF CONFORMITY

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

3.3 IDENTIFICATION AND IDENTITY ESTABLISHMENT UPON RENEWAL OF A QUALIFIED CERTIFICATE

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

3.4 IDENTIFICATION AND IDENTITY ESTABLISHMENT UPON SUSPENSION OF A QUALIFIED CERTIFICATE

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

3.5 IDENTIFICATION AND ESTABLISHMENT OF THE IDENTITY WHEN TERMINATING A

QUALIFIED CERTIFICATE

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

3.6 IDENTIFICATION AND ESTABLISHMENT OF THE IDENTITY AFTER TERMINATING A QUALIFIED CERTIFICATE

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

4 OPERATIONAL REQUIREMENTS

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

4.1 SUBMISSION OF A REQUEST FOR THE ISSUANCE OF A QUALIFIED CERTIFICATE

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

4.1.1 WHO CAN APPLY FOR A QUALIFIED CERTIFICATE

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

4.1.2 PROCESSING OF THE REQUEST FOR THE ISSUANCE OF A QUALIFIED CERTIFICATE AND THE RELATED OBLIGATIONS

4.1.2.1 USER CERTIFICATES

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

4.1.2.2 CERTIFICATES OF CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY

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

4.1.2.3 REQUEST FOR REGISTRATION OF USERS OF QUALIFIED TRUST SERVICES

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

4.1.2.4 RENEWAL OF A QUALIFIED CERTIFICATE, GENERATION OF A NEW KEY PAIR (REKEY) AND CHANGE OF A QUALIFIED CERTIFICATE

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

4.1.2.5 REQUEST FOR SUSPENSION AND TERMINATION OF A CERTIFICATE

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

4.2 PROCESSING OF THE REQUEST

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

4.2.1 PERFORMING IDENTIFICATION AND ESTABLISHING IDENTITY

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

4.2.2 ACCEPTANCE OR REJECTION OF A REQUEST

4.2.2.1 PROCESSING OF A REQUEST BY THE REGISTRATION AUTHORITY

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

4.2.2.2 PLACING A REQUEST WITH THE CERTIFICATION AUTHORITY FOR ISSUING A QUALIFIED CERTIFICATE

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

4.2.3 AWAITING FOR THE ISSUANCE OF A QUALIFIED CERTIFICATE

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

4.2.4 THE CERTIFICATION AUTHORITY AUTHORIZES DATA PROCESSING

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

4.3 ISSUANCE OF A QUALIFIED CERTIFICATE

4.3.1 PROCESSING

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

4.3.2 PROVIDING INFORMATION

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

4.4 ACCEPTANCE OF A QUALIFIED CERTIFICATE

4.4.1 CONFIRMATION FOR ACCEPTANCE OF A QUALIFIED CERTIFICATE

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

4.4.2 PUBLICATION OF A QUALIFIED CERTIFICATE

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

4.4.3 INFORMATION INTENDED FOR OTHER PARTIES

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

4.5 USE OF A QUALIFIED CERTIFICATE AND A KEY PAIR

4.5.1 BY USERS

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

4.5.2 BY RELYING PARTIES

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

4.6 RENEWAL OF A QUALIFIED CERTIFICATE

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

4.7 ISSUANCE OF A QUALIFIED CERTIFICATE BY GENERATING A NEW KEY PAIR (RE-KEY)

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

4.7.1 CIRCUMSTANCES UNDER WHICH ISSUANCE OF A QUALIFIED CERTIFICATE IS APPLIED BY GENERATING A NEW KEY PAIR (RE-KEY)

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

4.7.2 PERSONS AUTHORIZED TO REQUEST AN UPDATE OF A KEY PAIR

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

4.7.3 RE-KEY AND PROCESSING OF THE REQUEST

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

4.7.4 USER INFORMATION

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

4.7.5 CONFIRMATION OF ACCEPTANCE OF A NEW CERTIFICATE

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

4.7.6 PUBLICATION OF A NEW QUALIFIED CERTIFICATE

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

4.7.7 INFORMATION INTENDED FOR THE RELYING PARTIES

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

4.8 CHANGE IN A QUALIFIED CERTIFICATE

4.8.1 REASONS FOR THE CHANGE IN A QUALIFIED CERTIFICATE

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

4.8.2 PERSONS AUTHORIZED TO REQUEST A CHANGE OF A QUALIFIED CERTIFICATE?

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

4.8.3 PROCESSING OF THE REQUEST

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

4.8.4 USER INFORMATION

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

4.8.5 CONFIRMATION OF ACCEPTANCE OF A NEW QUALIFIED CERTIFICATE

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

4.8.6 PUBLICATION OF A NEW QUALIFIED CERTIFICATE

EVROTRUST, through the Operational Certification Authority, publishes the changed qualified certificate immediately in the Public Register/Repository.

4.8.7 INFORMATION INTENDED FOR THE RELYING PARTIES

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

4.9 SUSPENSION AND TERMINATION OF A QUALIFIED CERTIFICATE

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

4.9.1 CIRCUMSTANCES FOR TERMINATION OF A QUALIFIED CERTIFICATE

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

4.9.2 WHO MAY REQUIRE TERMINATION OF A QUALIFIED CERTIFICATE?

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

4.9.3 PROCEDURE FOR TERMINATION OF A QUALIFIED CERTIFICATE

4.9.3.1 PROCEDURE FOR TERMINATION OF A QUALIFIED END USER CERTIFICATE

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

4.9.3.2 PROCEDURE FOR TERMINATION OF A QUALIFIED CERTIFICATE BY THE CERTIFICATION AUTHORITY OR REGISTRATION AUTHORITY

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

4.9.4 GRACE PERIOD OF TERMINATION OF A QUALIFIED CERTIFICATE

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

4.9.5 TIME LIMITS FOR PROCESSING OF THE TERMINATION REQUEST

A request for termination of a qualified certificate shall be processed by EVROTRUST without undue delay.

4.9.6 CHECK OF THE CERTIFICATE REVOCATION LIST (CRL)

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

4.9.7 FREQUENCY OF ISSUING THE CERTIFICATE REVOCATION LIST (CRL)

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

4.9.8 MAXIMUM DELAY OF PUBLICATION OF CRL

Each CRL is published without undue delay as soon as it is created (usually automatically within a few minutes).

4.9.9 ONLINE VERIFICATION OF THE CERTIFICATE STATUS

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

4.9.10 REQUIREMENTS FOR ONLINE VERIFICATION OF THE CERTIFICATE STATUS

A real-time verification of the certificate status (through an OCSP protocol) can be performed via the Internet at the website of EVROTRUST: https://www.evrotrust.com.

4.9.11 SPECIAL REQUIREMENTS FOR A SECURITY BREACH OF THE KEY

In the event of a security breach of the private key (its disclosure) of the Certification Authority or other entities operating within EVROTRUST, EVROTRUST shall immediately inform the Relying Parties.

4.9.12 CIRCUMSTANCES FOR SUSPENSION OF A QUALIFIED CERTIFICATE

EVROTRUST, through its Operational Certification Authority, suspends a valid certificate under certain conditions and for a grace period until the reasons for the suspension are specified, but not longer than 72 hours.

4.9.13 PERSONS AUTHORIZED TO REQUEST THE SUSPENSION OF A QUALIFIED CERTIFICATE

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

4.9.14 PROCEDURE FOR SUSPENSION AND RESUMPTION OF A QUALIFIED CERTIFICATE

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

4.9.15 GRACE PERIOD OF SUSPENSION OF A QUALIFIED CERTIFICATE

EVROTRUST suspends a Qualified Website Authentication Certificate for a grace period after receipt of the request for suspension until the reasons for the suspension have been specified but no

longer than 72 hours.

4.9.16 RESUMPTION OF A SUSPENDED CERTIFICATE

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

4.9.17 PROCEDURE FOR RESUMPTION OF A QUALIFIED CERTIFICATE

The Registration authority resume a suspended certificate after receiving a request for resumption from a User and after a successful identification check and identity establishment

The Registration authority immediately resumes a suspended certificate after the grace period expires.

4.10 CHECKING THE CURRENT STATUS (STATUS) OF QUALIFIED CERTIFICATES

4.10.1 CHARACTERISTICS

Information on the status of certificates issued by EVROTRUST can be obtained from the CRL, published on the EVROTRUST Web site, via the Online Certificate Status Protocol (OCSP).

Trust services for checking the status of qualified certificates are available in a 24/7 mode (continuously operating).

4.10.2 ADDITIONAL FUNCTIONS

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

4.11 TERMINATION OF A CONTRACT FOR QUALIFIED TRUST SERVICES BY A USER

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

4.12 PRIVATE KEY ESCROW

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

5 CONTROL OVER THE PHYSICAL AND ORGANIZATIONAL SECURITY

5.1 PHYSICAL SECURITY CONTROL

The measures taken with regard to the physical protection of EVROTRUST are an element of the developed and implemented Information Security System, conforming to the requirements of ISO/IEC 27001:2013 and ISO / IEC 19011:2013.

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

5.1.1 PREMISES AND CONSTRUCTION OF PREMISES

EVROTRUST has specially designed and equipped areas with the highest degree of physical access control, which house the Certification Authority of EVROTRUST and all the central components of the infrastructure.

5.1.2 PHYSICAL ACCESS

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

5.1.3 STORAGE ON DATA MEDIA

All media containing software, data archives, or audit information are stored in a fireproof safe in a special archive room with access control. There is a system of physical and logical protection in the room with EVROTRUST's archive.

5.1.4 WASTE DISPOSAL

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

5.2 ORGANIZATIONAL CONTROL

All security procedures related to issuing, administering, and using Qualified Website Authentication Certificates are performed by trusted personnel of EVROTRUST.

EVROTRUST maintains a sufficient number of qualified employees who at every moment of its

activity ensure compliance with the applicable legislation and the company's internal rules and regulations.

5.2.1 TRUSTED ROLES

A detailed allocation of the functions and responsibilities of the personnel is set out in the EVROTRUST internal documents: job descriptions, establishment plan and corresponding internal operational procedures.

The allocation of functions is done in such a way as to minimize the risk of compromising, leakage of confidential information or the occurrence of a conflict of interest.

5.2.2 REQUIREMENTS FOR THE SEPARATION OF DUTIES

The trusted activities of EVROTRUST personnel are performed by different persons.

5.3 PERSONNEL CONTROL

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

5.3.1 REQUIREMENTS FOR THE TRAINING OF EVROTRUST PERSONNEL

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

5.4 RECORDING EVENTS AND MAINTAINING JOURNALS

Archived journals are kept for at least 20 (twenty) years.

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

5.4.1 VULNERABILITY AND EVALUATION

EVROTRUST classifies and maintains registers of all assets in accordance with the requirements of ISO/IEC 27001:2013. According to the "Security Policy" of EVROTRUST, an analysis is carried out for the vulnerability assessment of all internal procedures, applications and information systems. The analysis requirements may also be determined by an external institution authorized to audit

EVROTRUST.

The risk analysis shall be carried out at least once a year.

5.5 ARCHIVING

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

5.6 TERMINATION OF THE EVROTRUST ACTIVITY

5.6.1 REQUIREMENTS RELATING TO THE TRANSITION TO TERMINATION OF THE PROVIDER'S ACTIVITY

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

5.6.2 TRANSFER OF OPERATION TO ANOTHER PROVIDER OF QUALIFIED TRUST SERVICES

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

5.6.3 WITHDRAWAL OF A QUALIFIED STATUS OF A PROVIDER OR A QUALIFIED STATUS OF A RELEVANT SERVICE

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

6 MANAGEMENT AND CONTROL OVER THE TECHNICAL SECURITY

6.1 GENERATION AND INSTALLATION OF A KEY PAIR OF A CERTIFICATION AUTHORITY

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

6.1.1 GENERATION OF A KEY PAIR OF A NATURAL PERSON/LEGAL ENTITY

EVROTRUST uses algorithms that meet the requirements of ETSI TS 119 312.

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

6.1.1.1 REMOTE GENERATION OF A KEY PAIR

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

6.1.2 DELIVERY OF A PRIVATE KEY TO A USER

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

6.1.3 DELIVERY OF A PUBLIC KEY BY A USER TO A PROVIDER

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

6.1.4 KEY LENGTH

The length of a key pair for a qualified electronic signature is in accordance with ETSI TS 119 312 [14], the CABF Baseline Requirements Recommendation [24] and national legislation.

6.1.5 PUBLIC KEY PARAMETERS

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

6.2 PROTECTION OF A PRIVATE KEY AND CRYPTOGRAPHY MODULE CONTROL

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

6.2.1 CONTROL OVER THE USE AND STORAGE OF A PRIVATE KEY

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

6.2.2 STORAGE OF A PRIVATE KEY

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

6.2.3 METHOD FOR ACTIVATION OF A PRIVATE KEY

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

6.2.4 METHOD FOR DEACTIVATION OF A PRIVATE KEY

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

6.2.5 METHOD FOR DESTRUCTION OF A PRIVATE KEY

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

6.3 OTHER ASPECTS OF MANAGING A KEY PAIR

6.3.1 PUBLIC KEY ARCHIVING

The public keys of Users are contained in the Qualified Certificates issued to them, which are published in the Public Register on the EVROTRUST Web site and stored in a repository.

6.3.2 VALIDITY PERIOD OF A QUALIFIED CERTIFICATE AND USE OF KEYS

The period of use of public keys is determined by the value of the field in the certificate describing the validity of the public key.

6.4 DATA FOR ACTIVATION

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

6.4.1 GENERATION AND INSTALLATION OF DATA FOR ACTIVATION

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

6.4.2 PROTECTION OF DATA FOR ACTIVATION

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

6.5 SECURITY OF COMPUTER SYSTEMS

EVROTRUST uses only reliable and secure hardware and software that are part of the computer system of EVROTRUST.

6.6 SECURITY OF THE LIFE CYCLE OF THE TECHNOLOGICAL SYSTEM

Supervision of the functionality of the technological system is performed and it is ensured that it functions properly and in accordance with the delivered manufacturing configuration.

6.7 NETWORK SECURITY

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

7 PROFILES OF QUALIFIED CERTIFICATES, CRL AND OCSPS

The profiles of the User Qualified Certificates issued by EVROTRUST, the certificates of the Certification Authority (basic and operational) used in the provision of qualified trust services meet the following recommendations and requirements:

- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Publickey and attribute certificate frameworks;
- RFC 5280;
- RFC 6818;
- ETSI EN 319 412-1;
- ETSI EN 319 412-2 in case of issuance of a certificate for a natural person;
- ETSI EN 319 412-3 in case of issuance of a certificate for a legal entity;
- ETSI EN 319 412-4.

Qualified certificates for website authentication contain:

- an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;
- a set of data that uniquely describes EVROTRUST as a provider of qualified trust services that has issued the certificate, and the set shall comprise at least the Member State of establishment of the provider and:
  - for natural persons: at least the name of the person to whom the certificate was issued or a pseudonym. If a pseudonym is used, it shall be clearly indicated;
  - for legal entities: at least the name of the legal entity to whom the certificate was issued and, where applicable, the registration number as stated in the official records;

- the domain name(s) operated by the natural person or legal entity to whom the certificate was issued;
- details of the beginning and end of the certificate's period of validity;
- certificate identification code (serial number) that is unique for the provider of qualified trust services;
- an advanced electronic signature or advanced electronic seal of the issuing provider of qualified trust services;
- a place where the certificate supporting the advanced electronic signature or the advanced electronic seal of the issuing provider is available free of charge;
- the location of the certificate validity check services that can be used for making enquiries about the validity status of the qualified certificate.

7.1 PROFILE OF QUALIFIED EVROTRUST SSL DOMAIN VALIDATED CERTIFICATE:

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)=	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Validit to	[UTC end date and time of certificate validity]	
Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166
	CN= (commonName)	Domain name, IP or Resource name
Public Key Type/Length	RSA (2048 Bits)	
Subject Key Identifier	[Calculated value for issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name:	

	Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl
Authority Information Access	[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
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)
Subject Alternative Name	DNS Name=[Domain name or IP]
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)
QCStatements	id-etsi-qcs-**QcCompliance** (oid=0.4.0.1862.1.1) id-etsi-qcs-**QcLimitValue** (0.4.0.1862.1.2) — BGN 400 id-etsi-qcs-**QcType** (oid=0.4.0.1862.1.6) — id-etsi-qct-**web** (oid=0.4.0.1862.1.6.3) id-etsi-qcs-**QcPDS** (oid=0.4.0.1862.1.5) — PdsLocations PdsLocation=https://www.evrotrust.com/pds/pds_en.pdf language=en

7.2 PROFILE OF QUALIFIED EVROTRUST SSL ORGANIZATION VALIDATED CERTIFICATE:

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)=	NTRBG-203397356
	C=	BG
Valid from	[UTC start date and time of certificate validity]	
Validit to	[UTC end date and time of certificate validity]	
Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166
	CN= (commonName)	Domain name, IP or Resource name
	O*= (organizationName)	Name of the person: Full name under the registration or act of registration of the legal entity with which the natural person is associated.
	2.5.4.97*= (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: - VARBG-123456789 – VAT; - NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity with which the natural person is associated.
Public Key Type/Length	RSA (2048 Bits)	
Subject Key Identifier	[Calculated value for issued certificate]	
Authority Key Identifier	Key ID=7F:3E:64:59:85:2B:DD:23:29:C2:01:E7:CB:C3:69:C0:87:93:2B:08	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.evrotrust.com/crl/EvrotrustRSAOperationalCA.crl	
Authority Information	[1]Authority Info Access	

<table>
<tr><td>Access</td><td>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>Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)</td></tr>
<tr><td>Subject Alternative Name</td><td>DNS Name=[Domain name or IP]</td></tr>
<tr><td>Subject Alternative Name</td><td>DNS Name=[Domain name or IP]</td></tr>
<tr><td>Certificate Policies</td><td>[1]Certificate Policy:
Policy Identifier=1.3.6.1.4.1.47272.2.4.2
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CPS
Qualifier:
http://www.evrotrust.com/cps</td></tr>
<tr><td>Key Usage (critical)</td><td>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-Legal* (oid=0.4.0.194121.1.2)</td></tr>
<tr><td colspan="2">id-etsi-qcs-QcCompliance (oid=0.4.0.1862.1.1)</td></tr>
<tr><td>id-etsi-qcs-QcLimitValue (0.4.0.1862.1.2)</td><td>BGN 400</td></tr>
<tr><td>id-etsi-qcs-QcType (oid=0.4.0.1862.1.6)</td><td>id-etsi-qct-web (oid=0.4.0.1862.1.6.3)</td></tr>
<tr><td>id-etsi-qcs-QcPDS (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>

7.3 PROFILE OF THE CERTIFICATE REVOCATION LIST (CRL)

The profile is described in the document "Certification Practice Statement for Qualified Trust Services".

7.4 OCSP/ONLINE CERTIFICATE STATUS PROTOCOL

The profile is described in the document "Certification Practice Statement for Qualified Trust Services".

8 AUDIT

EVROTRUST has an independent external auditor check its work. During the audit the conformity of EVROTRUST's activity with the following normative documents is checked:

- Regulation (EU) No 910/2014;
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;
- ETSI EN 319 411-2 v2.1.1 (2016-02); Part 2: Requirements for trust service providers issuing EU qualified certificates;
- ETSI EN 319 421 v.1.1.1 (2016-08); Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

8.1 FREQUENCY OF THE AUDIT

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

8.2 QUALIFICATION OF THE AUDITORS

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

8.3 RELATIONSHIPS OF THE AUDITORS WITH THE PROVIDER

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

8.4 SCOPE OF THE AUDIT

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

8.5 ACTIONS TAKEN AS A RESULT OF AUDIT

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

8.6 STORAGE OF AUDIT RESULTS

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

9 OTHER BUSINESS AND LEGAL ISSUES

9.1 PRICES AND FEES

EVROTRUST maintains the document "Tariff for trust, information, cryptographic and advisory services provided" on its website at https://www.evrotrust.com.

9.1.1 REMUNERATION

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

9.1.2 REMUNERATION FOR TRUST, CRYPTOGRAPHIC, INFORMATION AND ADVISORY SERVICES PROVIDED

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

9.1.3 INVOICING

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

9.1.4 RETURN OF A CERTIFICATE AND RECOVERY OF PAYMENT

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

9.1.5 FREE SERVICES

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

9.2 FINANCIAL RESPONSIBILITIES

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

9.2.1 INSURANCE OF THE BUSINESS ACTIVITY

EVROTRUST concludes compulsory insurance of its activity as a registered Provider of Qualified Trust Services.

9.2.2 INSURANCE COVERAGE

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

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

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

9.3.2 NON-CONFIDENTIAL INFORMATION

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

9.3.3 PROTECTION OF CONFIDENTIAL INFORMATION

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

9.4 PROTECTION OF PERSONAL DATA

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

9.5 INTELLECTUAL PROPERTY RIGHTS

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

9.5.1 PRIVACY POLICY

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

9.5.2 INFORMATION TREATED AS PERSONAL

Any information on users, that is not publicly available through the content of the issued certificates, repository, or online through the Certificate Revocation List (CRL), is treated as personal.

9.5.3 INFORMATION THAT IS NOT CONSIDERED PERSONAL

All the information disclosed in the certificates is considered to be non-personal, unless expressly provided otherwise in the Personal Data Protection Act.

9.5.4 RESPONSIBILITY FOR PROTECTION OF PERSONAL DATA

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

9.5.5 CONSENT TO USE PERSONAL DATA

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

9.6 INTELLECTUAL PROPERTY RIGHTS

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

9.6.1 DATA PROPERTY RIGHTS IN QUALIFIED CERTIFICATES

EVROTRUST retains all intellectual property rights of the data included in Qualified Certificates.

9.6.2 PROPERTY RIGHTS OF NAMES AND TRADE MARKS

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

9.6.3 PROPERTY RIGHTS OF A KEY PAIR

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

9.7 GENERAL

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

9.7.1 OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF EVROTRUST

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

9.7.2 OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF REGISTRATION AUTHORITY

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

9.7.3 OBLIGATIONS OF USERS

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

9.7.4 DUE DILIGENCE OF A RELYING PARTY

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

9.7.5 OBLIGATIONS OF OTHER PARTIES

9.7.5.1 OBLIGATIONS OF THE QUALIFIED VALIDATION AUTHORITY

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

9.7.5.2 OBLIGATIONS OF THE QUALIFIED OPERATIONAL CERTIFICATION AUTHORITY

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

9.7.5.3 OBLIGATIONS OF EVROTRUST TO THE PUBLIC REGISTERS/REPOSITORY

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

9.8 DISCLAIMER

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

9.9 LIMITATIONS OF RESPONSIBILITY

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

9.10 RESPONSIBILITY OF A NATURAL PERSON/LEGAL ENTITY

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

9.10.1 RESPONSIBILITY OF A NATURAL PERSON/LEGAL ENTITY TO EVROTRUST

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

9.11 DURATION AND TERMINATION OF "CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR WEBSITE AUTHENTICATION"

9.11.1 DURATION

This Policy shall enter into force upon its approval by the Board of Directors of EVROTRUST and its publication in the Public Register/Repository of EVROTRUST.

The provisions in this document are valid until the next version of the "Certificate Policy for Qualified Certification Services for Website Authentication" is published in the repository, available on the website of EVROTRUST.

9.11.2 TERMINATION

The policy is in force (has a current status) until the approval and publication of a new version.

Upon termination of the activity of EVROTRUST, the validity of the Policy as well as the provisions contained in this document shall be terminated.

EVROTRUST keeps all previous versions/revisions of this document duly and securely.

9.11.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this document, Users and Relying parties shall remain bound in terms of issued user qualified certificates for the remainder of the period of validity of these certificates.

9.12 NOTES AND COMMUNICATIONS BETWEEN THE PARTIES

The parties mentioned in this Policy can communicate under different methods. This document enables the exchange of information by means of ordinary mail, e-mail, fax, telephone, via mobile applications and network protocols (e.g. TCP/IP, HTTP), etc.

The means can be chosen depending on the type of information.

Information on any breakthrough in the security of the private keys of the Certification Authorities should be published on the EVROTRUST web site, which will make it available to all interested parties.

9.13 AMENDMENTS TO "CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR WEBSITE AUTHENTICATION"

The amendments to the Policy may result from observed errors, updates, and proposals by the interested parties. In the event of an invalid clause in this document, the validity of the entire document is retained and the contract with the User is not violated.

EVROTRUST may make editorial changes to this document, that do not affect the content of the rights and obligations contained therein.

Changes that lead to a new version/revision of the document are published on the EVROTRUST website.

9.14 SETTLEMENT OF DISPUTES

The subject of disputes can only be inconsistencies or contradictions between the parties bound by agreements that relate to this Policy.

Disputes or complaints regarding the use of certificates provided by EVROTRUST will be resolved in the spirit of goodwill. Requests must be made in writing at the address of EVROTRUST:

Evrotrust Technologies AD
Sofia, 101 Tsarigradsko Shose Blvd.
Business Centre “AKTIV”, 6th floor
Telephone, Fax: + 359 2 448 58 58

Complaints will be dealt with by the legal department of EVROTRUST. The complainant will receive a reply within 2 working days of receiving the complaint. In the event that no dispute resolution is found within 30 days of the commencement of the settlement procedure, the parties may refer the dispute to a court.

9.15 APPLICABLE LAW

For all matters not covered by this document the provisions of the Bulgarian legislation shall apply.

9.16 COMPLIANCE WITH THE APPLICABLE LAW

This document has been developed in accordance with the national law.

9.17 OTHER PROVISIONS

The policy does not specify any other provisions.

9.18 COMPLIANCE WITH STANDARDS AND STANDARDIZATION 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.
- ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 412-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI);

Certificate Profiles; Part 1: Overview and common data structures.

- ETSI EN 319 412-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons; (Replaces ETSI TS 102 280).
- ETSI EN 319 412-3 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons (Replaces ETSI TS 101 861).
- ETSI EN 319 412-4 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- ETSI TS 119 312 V1.1.1 (2014-11); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- MSZ/ISO/IEC 15408-2002 "Information Technology - Methods and Means of a Security - Evaluation Criteria for IT Security".
- ISO/IEC 19790:2012: "Information technology – Security techniques – Security requirements for cryptographic modules".
- IETF RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 1999.
- IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.
- IETF RFC 4043: Internet X.509 Public Key Infrastructure - Permanent Identifier, May 2005.
- IETF RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, May 2008.
- IETF RFC 6818: Updates to the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, January 2013.
- IETF RFC 6960: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP), June 2013.
- ITU X.509 Information technology - Open Systems Interconnection - The Directory: Publickey and attribute certificate frameworks.
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.3.0. CA/Browser Forum, https://cabforum.org/wp-content/uploads/CAB-Forum-BR-1.3.0.pdf, 2015.
- FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.
- CEN Workgroup Agreement CWA 14167-2: Cryptographic module for CSP signing operations with backup - Protection profile - CMCSOB PP.

Registration of changes																					
Page																					
Valid change																					