

**POLICY
FOR QUALIFIED CERTIFICATION SERVICES
FOR WEBSITE AUTHENTICATION**

CONTENTS

1.1	REVIEW	8
1.2	NAME AND IDENTIFICATION OF THE DOCUMENT	9
1.3	PARTICIPANTS IN THE EVROTRUST INFRASTRUCTURE.....	11
1.3.1	CERTIFICATION AUTHORITIES	11
1.3.2	REGISTRATION AUTHORITY	12
1.3.3	USERS	12
1.3.4	RELYING PARTIES	12
1.3.5	OTHER PARTICIPANTS	12
1.4	USE OF QUALIFIED CERTIFICATES	13
1.4.1	USE OF EV CERTIFICATES	13
1.4.2	RECOMMENDED APPLICATION SCOPE	14
1.4.3	BAN ON THE USE OF QUALIFIED CERTIFICATES.....	14
1.5	POLICY MANAGEMENT.....	14
1.5.1	ORGANIZATION MANAGING THE POLICY	14
1.5.2	CONTACT PERSON	15
1.5.3	POLICY AND PRACTICE MANAGEMENT	15
1.5.4	PROCEDURES FOR THE PRACTICE APPROVAL	15
1.6	DEFINITIONS AND ABBREVIATIONS.....	16
1.6.1	DEFINITIONS.....	16
1.6.2	ABBREVIATIONS	23
2	RESPONSIBILITY FOR PUBLISHING AND THE REPOSITORY	24
2.1	REPOSITORY	24
2.2	INFORMATION PUBLISHED BY EVROTRUST	24
2.3	FREQUENCY OF PUBLICATION.....	25
2.4	ACCESS TO PUBLICATIONS	26
3	NAMES	26
3.1	TYPES OF NAMES	26
3.2	NECESSITY OF MEANINGFUL NAMES	27
3.3	ANONYMITY OR PSEUDONYMS OF USERS	27
3.4	RULES FOR INTERPRETATION OF DIFFERENT NAME FORMS	27
3.5	UNIQUENESS OF NAMES	27
3.6	ALTERNATIVE NAMES.....	27
3.7	NAME OF A WEB SERVER (SUBJECT).....	28
3.8	RECOGNITION, CERTIFICATION OF AUTHENTICATION AND ROLE OF THE TRADEMARK. DISPUTE SETTLEMENT PROCEDURE.....	30
4	INITIAL REGISTRATION AND IDENTIFICATION/ESTABLISHMENT OF IDENTITY	30
4.1	VERIFICATION OF PRIVATE KEY POSSESSION	31
4.2	ORGANIZATION AND DOMAIN IDENTITY VERIFICATION	31
4.2.1	IDENTITY VERIFICATION	31
4.2.2	TRADE NAME/DBA	32
4.2.3	COUNTRY VERIFICATION	32
4.2.4	DOMAIN CERTIFICATION OR CONTROL VERIFICATION	33
4.2.5	CERTIFICATION FOR IP ADDRESS.....	40
4.2.6	ACCURACY OF THE DATA SOURCE	43
4.2.7	CAA RECORDS.....	43
4.3	CERTIFICATION OF THE IDENTITY OF A NATURAL PERSON.....	44
4.4	VERIFICATION OF THE POWER OF REPRESENTATION	45

4.5	SPECIAL ATTRIBUTES.....	45
4.6	UNCONFIRMED INFORMATION.....	45
4.7	INTEROPERABILITY CRITERIA	45
4.8	IDENTIFICATION AND IDENTITY ESTABLISHMENT UPON RENEWAL OF A QUALIFIED CERTIFICATE	46
4.9	IDENTIFICATION AND IDENTITY ESTABLISHMENT UPON SUSPENSION OF A QUALIFIED CERTIFICATE	46
4.10	IDENTIFICATION AND ESTABLISHMENT OF THE IDENTITY WHEN TERMINATING A QUALIFIED CERTIFICATE.....	46
4.11	IDENTIFICATION AND ESTABLISHMENT OF THE IDENTITY AFTER TERMINATING A QUALIFIED CERTIFICATE.....	46
5	REQUIREMENTS FOR REGISTRATION AND VERIFICATION OF AN APPLICANT FOR THE ISSUANCE OF EV CERTIFICATES.....	46
5.1	IDENTIFICATION AND ESTABLISHMENT OF IDENTITY	47
5.2	GENERAL VERIFICATION REQUIREMENTS IN ACCORDANCE WITH CA/BROWSER FORUM.....	47
5.2.1	OVERVIEW OF ELIGIBLE VERIFICATION METHODS.....	48
5.2.2	DISCLOSURE OF VERIFICATION SOURCES	48
5.3	VERIFICATION OF THE APPLICANT'S LEGAL EXISTENCE AND IDENTITY	49
5.3.1	VERIFICATION REQUIREMENTS	49
5.3.2	ELIGIBLE VERIFICATION METHODS	50
5.4	VERIFICATION OF THE APPLICANT'S LEGAL EXISTENCE AND IDENTITY - ASSUMED (ALTERNATIVE) NAME	54
5.4.1	VERIFICATION REQUIREMENTS	54
5.4.2	ELIGIBLE VERIFICATION METHOD	54
5.5	VERIFICATION OF THE APPLICANT'S PHYSICAL EXISTENCE.....	55
5.5.1	THE APPLICANT'S ADDRESS AND PLACE OF BUSINESS.....	55
5.6	VERIFICATION OF THE COMMUNICATION METHOD.....	57
5.6.1	VERIFICATION REQUIREMENTS	57
5.6.2	ELIGIBLE VERIFICATION METHODS	57
5.7	VERIFICATION OF THE APPLICANT'S OPERATIONAL EXISTENCE.....	57
5.7.1	VERIFICATION REQUIREMENTS	57
5.7.2	ELIGIBLE VERIFICATION METHODS	57
5.8	VERIFICATION OF THE APPLICANT'S DOMAIN NAME.....	58
5.8.1	VERIFICATION REQUIREMENTS	58
5.9	VERIFICATION OF THE NAME, TITLE AND AUTHORITY OF THE CONTRACT SIGNATORY AND THE CERTIFICATE APPROVER.....	58
5.9.1	VERIFICATION REQUIREMENTS	58
5.9.2	ELIGIBLE VERIFICATION METHODS - NAME, TITLE AND AGENCY.....	59
5.9.3	ELIGIBLE VERIFICATION METHODS - COMPETENT AUTHORITY	60
5.9.1	RE-AUTHORIZED CERTIFICATE APPROVER	62
5.10	VERIFICATION OF SIGNATURE ON A USER CONTRACT AND EV CERTIFICATE APPLICATIONS.....	62
5.10.1	VERIFICATION REQUIREMENTS	62
5.10.2	ELIGIBLE SIGNATURE VERIFICATION METHODS	63
5.11	VERIFICATION OF APPROVAL OF AN EV CERTIFICATE APPLICATION.....	63
5.11.1	VERIFICATION REQUIREMENTS	63
5.11.2	ELIGIBLE VERIFICATION METHODS	64
5.12	VERIFICATION OF CERTAIN SOURCES OF INFORMATION	64

5.12.1 VERIFICATION OF LEGAL OPINION	64
5.12.2 VERIFICATION OF ACCOUNTING LETTER.....	65
5.12.3 FACE-TO-FACE VERIFICATION.....	67
5.12.4 INDEPENDENT CONFIRMATION BY THE APPLICANT	68
5.12.5 RELIABLE INDEPENDENT INFORMATION SOURCE	70
5.12.6 RELIABLE GOVERNMENTAL INFORMATION SOURCE.....	70
5.12.7 RELIABLE SOURCE OF GOVERNMENT TAX INFORMATION	71
5.13 OTHER VERIFICATION REQUIREMENTS.....	71
5.13.1 REFUSAL LISTS AND OTHER LEGAL BLOCKING LISTS.....	71
5.13.2 PARENT / SUBSIDIARY / AFFILIATE RELATIONS	71
5.14 FINAL CROSS-CORRELATION AND DUE DILIGENCE	72
5.15 REQUIREMENTS FOR THE RE-USE OF EXISTING DOCUMENTATION.....	73
5.15.1 VERIFICATION FOR EXISTING SUBSCRIBERS	73
5.15.2 REQUESTS FOR RE-ISSUE.....	74
5.15.3 VALIDITY PERIOD OF THE VERIFIED DATA.....	74
6 OPERATIONAL REQUIREMENTS	75
6.1 SUBMISSION OF A REQUEST FOR THE ISSUANCE OF A QUALIFIED CERTIFICATE	75
6.1.1 WHO CAN APPLY FOR A QUALIFIED CERTIFICATE	75
6.1.2 PROCESSING OF THE REQUEST FOR THE ISSUANCE OF A QUALIFIED CERTIFICATE AND THE RELATED OBLIGATIONS	75
6.2 PROCESSING OF THE REQUEST	77
6.2.1 PERFORMING IDENTIFICATION AND ESTABLISHING IDENTITY.....	77
6.2.2 ACCEPTANCE OR REJECTION OF A REQUEST	77
6.2.3 AWAITING FOR THE ISSUANCE OF A QUALIFIED CERTIFICATE	77
6.2.4 THE CERTIFICATION AUTHORITY AUTHORIZES DATA PROCESSING	77
6.3 ISSUANCE OF A QUALIFIED CERTIFICATE	78
6.3.1 PROCESSING	78
6.3.2 PROVIDING INFORMATION	78
6.4 ACCEPTANCE OF A QUALIFIED CERTIFICATE	78
6.4.1 CONFIRMATION FOR ACCEPTANCE OF A QUALIFIED CERTIFICATE	78
6.4.2 PUBLICATION OF A QUALIFIED CERTIFICATE	78
6.4.3 INFORMATION INTENDED FOR OTHER PARTIES	78
6.5 USE OF A QUALIFIED CERTIFICATE AND A KEY PAIR	78
6.5.1 BY USERS	78
6.5.2 BY RELYING PARTIES	79
6.6 RENEWAL OF A QUALIFIED CERTIFICATE	79
6.7 ISSUANCE OF A QUALIFIED CERTIFICATE BY GENERATING A NEW KEY PAIR (RE-KEY) 79	
6.7.1 CIRCUMSTANCES UNDER WHICH ISSUANCE OF A QUALIFIED CERTIFICATE IS APPLIED BY GENERATING A NEW KEY PAIR (RE-KEY).....	79
6.7.2 PERSONS AUTHORIZED TO REQUEST AN UPDATE OF A KEY PAIR	79
6.7.3 RE-KEY AND PROCESSING OF THE REQUEST	79
6.7.4 USER INFORMATION.....	80
6.7.5 CONFIRMATION OF ACCEPTANCE OF A NEW CERTIFICATE	80
6.7.6 PUBLICATION OF A NEW QUALIFIED CERTIFICATE.....	80
6.7.7 INFORMATION INTENDED FOR THE RELYING PARTIES.....	80
6.8 CHANGE IN A QUALIFIED CERTIFICATE	80
6.8.1 REASONS FOR THE CHANGE IN A QUALIFIED CERTIFICATE	80
6.8.2 PERSONS AUTHORIZED TO REQUEST A CHANGE OF A QUALIFIED CERTIFICATE?	81
6.8.3 PROCESSING OF THE REQUEST.....	81
6.8.4 USER INFORMATION.....	81
6.8.5 CONFIRMATION OF ACCEPTANCE OF A NEW QUALIFIED CERTIFICATE	81

6.8.6	PUBLICATION OF A NEW QUALIFIED CERTIFICATE	81
6.8.7	INFORMATION INTENDED FOR THE RELYING PARTIES	81
6.9	SUSPENSION AND TERMINATION OF A QUALIFIED CERTIFICATE	81
6.9.1	CIRCUMSTANCES FOR TERMINATION OF A QUALIFIED CERTIFICATE	82
6.9.2	WHO MAY REQUIRE TERMINATION OF A QUALIFIED CERTIFICATE?	82
6.9.3	PROCEDURE FOR TERMINATION OF A QUALIFIED CERTIFICATE	83
6.9.4	GRACE PERIOD OF TERMINATION OF A QUALIFIED CERTIFICATE	84
6.9.5	TIME LIMITS FOR PROCESSING OF THE TERMINATION REQUEST	85
6.9.6	CHECK OF THE CERTIFICATE REVOCATION LIST (CRL)	86
6.9.7	FREQUENCY OF ISSUING THE CERTIFICATE REVOCATION LIST (CRL).....	86
6.9.8	MAXIMUM DELAY OF PUBLICATION OF CRL.....	86
6.9.9	ONLINE VERIFICATION OF THE CERTIFICATE STATUS	86
6.9.10	REQUIREMENTS FOR ONLINE VERIFICATION OF THE CERTIFICATE STATUS.....	87
6.9.11	SPECIAL REQUIREMENTS FOR A SECURITY BREACH OF THE KEY	87
6.9.12	CIRCUMSTANCES FOR SUSPENSION OF A QUALIFIED CERTIFICATE	87
6.9.13	PERSONS AUTHORIZED TO REQUEST THE SUSPENSION OF A QUALIFIED CERTIFICATE	87
6.9.14	PROCEDURE FOR SUSPENSION AND RESUMPTION OF A QUALIFIED CERTIFICATE.....	88
6.9.15	GRACE PERIOD OF SUSPENSION OF A QUALIFIED CERTIFICATE	88
6.9.16	RESUMPTION OF A SUSPENDED CERTIFICATE	88
6.9.17	PROCEDURE FOR RESUMPTION OF A QUALIFIED CERTIFICATE	88
6.10	CHECKING THE CURRENT STATUS (STATUS) OF QUALIFIED CERTIFICATES.....	88
6.10.1	CHARACTERISTICS	88
6.10.2	ADDITIONAL FUNCTIONS	88
6.11	TERMINATION OF A CONTRACT FOR QUALIFIED TRUST SERVICES BY A USER	89
6.12	PRIVATE KEY ESCROW	89
7	CONTROL OVER THE PHYSICAL AND ORGANIZATIONAL SECURITY	89
7.1	PHYSICAL SECURITY CONTROL	90
7.1.1	PREMISES AND CONSTRUCTION OF PREMISES	90
7.1.2	PHYSICAL ACCESS	91
7.1.3	STORAGE ON DATA MEDIA	91
7.1.4	WASTE DISPOSAL.....	91
7.2	ORGANIZATIONAL CONTROL	91
7.2.1	TRUSTED ROLES	91
7.2.2	REQUIREMENTS FOR THE SEPARATION OF DUTIES	92
7.3	PERSONNEL CONTROL	92
7.3.1	REQUIREMENTS FOR THE TRAINING OF EVROTRUST PERSONNEL	92
7.4	RECORDING EVENTS AND MAINTAINING JOURNALS	93
7.4.1	EVENT RECORDS	93
7.4.2	KEEPING JOURNALS	94
7.4.3	VULNERABILITY AND EVALUATION	94
7.5	ARCHIVING	95
7.6	COMPROMISE AND DISASTER RECOVERY.....	95
7.7	TERMINATION OF THE EVROTRUST ACTIVITY	96
7.7.1	REQUIREMENTS RELATING TO THE TRANSITION TO TERMINATION OF THE PROVIDER'S ACTIVITY.....	96
7.7.2	TRANSFER OF OPERATION TO ANOTHER PROVIDER OF QUALIFIED TRUST SERVICES	96
7.7.3	WITHDRAWAL OF A QUALIFIED STATUS OF A PROVIDER OR A QUALIFIED STATUS OF A RELEVANT SERVICE	96
8	MANAGEMENT AND CONTROL OVER THE TECHNICAL SECURITY	96
8.1	GENERATION AND INSTALLATION OF A KEY PAIR OF A CERTIFICATION AUTHORITY.....	96

8.1.1	GENERATION OF A KEY PAIR OF A NATURAL PERSON/LEGAL ENTITY	97
8.1.2	DELIVERY OF A PRIVATE KEY TO A USER	98
8.1.3	DELIVERY OF A PUBLIC KEY BY A USER TO A PROVIDER	98
8.1.4	KEY LENGTH	98
8.1.5	PUBLIC KEY PARAMETERS	98
8.2	PROTECTION OF A PRIVATE KEY AND CRYPTOGRAPHY MODULE CONTROL	98
8.2.1	CONTROL OVER THE USE AND STORAGE OF A PRIVATE KEY	98
8.2.2	SORAGE OF A PRIVATE KEY	98
8.2.3	METHOD FOR ACTIVATION OF A PRIVATE KEY	98
8.2.4	METHOD FOR DEACTIVATION OF A PRIVATE KEY	99
8.2.5	METHOD FOR DESTRUCTION OF A PRIVATE KEY	99
8.3	OTHER ASPECTS OF MANAGING A KEY PAIR	99
8.3.1	PUBLIC KEY ARCHIVING	99
8.3.2	VALIDITY PERIOD OF A QUALIFIED CERTIFICATE AND USE OF KEYS	99
8.4	DATA FOR ACTIVATION	99
8.4.1	GENERATION AND INSTALLATION OF DATA FOR ACTIVATION	99
8.4.2	PROTECTION OF DATA FOR ACTIVATION	100
8.5	SECURITY OF COMPUTER SYSTEMS	100
8.6	SECURITY OF THE LIFE CYCLE OF THE TECHNOLOGICAL SYSTEM	100
8.7	NETWORK SECURITY	100
9	PROFILES OF QUALIFIED CERTIFICATES, CRL AND OCSPS	100
9.1	PROFILE OF A QUALIFIED ORGANIZATION WEBSITE CERTIFICATE OF AUTHENTICITY „EVROTRUST SSL ORGANIZATION VALIDATED CERTIFICATE“	101
9.2	PROFILE OF A QUALIFIED CERTIFICATE FOR AUTHENTICITY OF WEBSITE WITH EXTENDED VALIDATION „EVROTRUST SSL EV CERTIFICATE“	103
9.3	PROFILE OF A QUALIFIED CERTIFICATE FOR AUTHENTICITY OF WEBSITE „EVROTRUST SSL PSD2 CERTIFICATE“	105
9.4	PROFILE OF QUALIFIED CERTIFICATE FOR DOMAIN WEBSITE AUTHORITY „EVROTRUST SSL DOMAIN VALIDATED CERTIFICATE“	107
9.5	PROFILE OF THE CERTIFICATE REVOCATION LIST (CRL)	108
9.6	OCSP / ONLINE CERTIFICATE STATUS PROTOCOL	108
10	AUDIT	108
10.1	FREQUENCY OF THE AUDIT	109
10.2	QUALIFICATION OF THE AUDITORS	109
10.3	RELATIONSHIPS OF THE AUDITORS WITH THE PROVIDER	109
10.4	SCOPE OF THE AUDIT	109
10.5	ACTIONS TAKEN AS A RESULT OF AUDIT	109
10.6	STORAGE OF AUDIT RESULTS	109
11	OTHER BUSINESS AND LEGAL ISSUES	109
11.1	PRICES AND FEES	109
11.1.1	REMUNERATION	109
11.1.2	REMUNERATION FOR TRUST, CRYPTOGRAPHIC, INFORMATION AND ADVISORY SERVICES PROVIDED	110
11.1.3	INVOICING	110
11.1.4	RETURN OF A CERTIFICATE AND RECOVERY OF PAYMENT	110
11.1.5	FREE SERVICES	110
11.2	FINANCIAL RESPONSIBILITIES	110
11.2.1	INSURANCE OF THE BUSINESS ACTIVITY	110
11.2.2	INSURANCE COVERAGE	110

11.3	CONFIDENTIALITY OF BUSINESS INFORMATION	110
11.3.1	SCOPE OF CONFIDENTIAL INFORMATION	111
11.3.2	NON-CONFIDENTIAL INFORMATION	111
11.3.3	PROTECTION OF CONFIDENTIAL INFORMATION	111
11.4	PERSONAL DATA PRIVACY.....	111
11.5	INTELLECTUAL PROPERTY RIGHTS	111
11.5.1	PRIVACY POLICY.....	111
11.5.2	INFORMATION TREATED AS PERSONAL.....	111
11.5.3	INFORMATION THAT IS NOT CONSIDERED PERSONAL.....	112
11.5.4	RESPONSIBILITY FOR PROTECTION OF PERSONAL DATA	112
11.5.5	CONSENT TO USE PERSONAL DATA.....	112
11.6	INTELLECTUAL PROPERTY RIGHTS	112
11.6.1	DATA PROPERTY RIGHTS IN QUALIFIED CERTIFICATES	112
11.6.2	PROPERTY RIGHTS OF NAMES AND TRADE MARKS	112
11.6.3	PROPERTY RIGHTS OF A KEY PAIR	112
11.7	GENERAL.....	112
11.7.1	OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF EVROTRUST	113
11.7.2	OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF REGISTRATION AUTHORITY	114
11.7.3	OBLIGATIONS OF USERS	114
11.7.4	DUE CARE OF A RELYING PARTY	115
11.7.5	OBLIGATIONS OF OTHER PARTIES	115
11.8	DISCLAIMER.....	115
11.9	LIMITATIONS OF RESPONSIBILITY	115
11.10	RESPONSIBILITY OF A NATURAL PERSON/LEGAL ENTITY	115
11.10.1	RESPONSIBILITY OF A NATURAL PERSON/LEGAL ENTITY TO EVROTRUST	116
11.11	DURATION AND TERMINATION OF "CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR WEBSITE AUTHENTICATION"	116
11.11.1	DURATION	116
11.11.2	TERMINATION	116
11.11.3	EFFECT OF TERMINATION AND SURVIVAL	116
11.12	NOTES AND COMMUNICATIONS BETWEEN THE PARTIES	116
11.13	AMENDMENTS TO "CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR WEBSITE AUTHENTICATION"	117
11.14	SETTLEMENT OF DISPUTES.....	117
11.15	APPLICABLE LAW.....	117
11.16	COMPLIANCE WITH THE APPLICABLE LAW	117
11.17	OTHER PROVISIONS	118
11.18	COMPLIANCE WITH STANDARDS AND STANDARDIZATION DOCUMENTS:	118

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 issuance, 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" and complies with the requirements of DIRECTIVE (EU)

2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 on payment services in the internal market amending Directives 2002/65 / EC, 2009/110 / EC and 2013/36 / EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64 / EC.

The policy complies with the following documents:

- ETSI EN 319 411-2 „Policy and security requirements for Trust Service Providers issuing certificates. Requirements for trust service providers issuing EU qualified certificates“;
- ETSI EN 319 401: „Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers“;
- ETSI EN 319 412-1: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“;
- ETSI EN 319 412-2: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“;
- ETSI EN 319 412-3: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons“;
- ETSI EN 319 412-5: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements“;
- ETSI TS 101 456: „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates“.
- ETSI TS 119 495: „Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366“;

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.

Domain Validation Certificate Policy (DV) identifier has the policy OID =

OID=1.3.6.1.4.1.47272.2.4.1, 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
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)
Evrotrust SSL EV Certificate	1.3.6.1.4.1.47272.2.5 (corresponds to a policy with OID = OID=0.4.0.2042.1.4)
Evrotrust SSL PSD2 Certificate	1.3.6.1.4.1.47272.2.5.1 (corresponds to a policy with OID=0.4.0.2042.1.4)

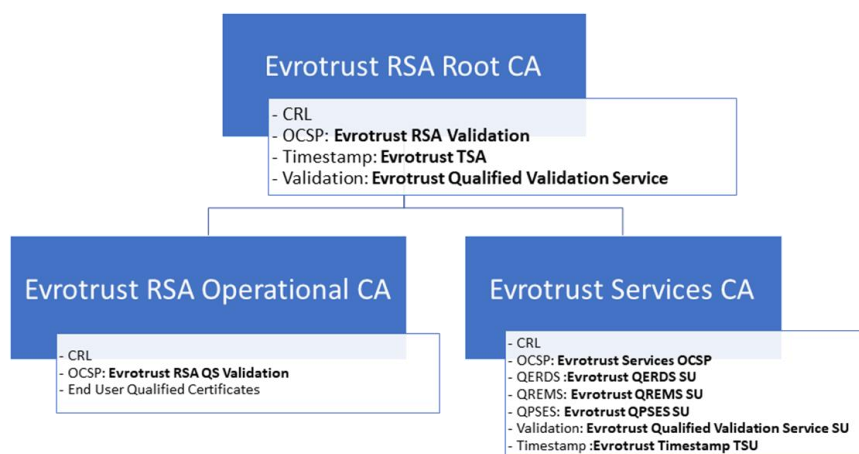
Evrotrust ensures that it does not change the object identifier of this document as well as the object identifiers of policies, practices and other referral documents. If there is an extension/update in policy and practice that will not affect previously issued certificates, Evrotrust presents a new object identifier that covers the new certificates or extended/updated ones. Evrotrust follows an internal OID management procedure.

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

The hierarchy of the certification authorities of Evrotrust is described in item 1.5.1.1 of the document entitled "Certification Practice Statement for Qualified Trust Services"



1.3.1.1 ROOT 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 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

A description of the use and applicability of qualified certificates can be found in the document "Certification Practice Statement for Qualified Trust Services".

The proper use of certificates aims to provide users with effective and secure electronic communication, while at the same time building their confidence in the reliability of certificates. The use of reliable certificates contributes to informing users and helps them make decisions.

This Policy serves to inform users and help them make informed decisions when relying on Evrotrust certificates.

Evrotrust provides termination information for both user and operational 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 USE OF EV CERTIFICATES

EV certificates are designed to establish web-based channels for data communication via TLS/SSL protocols and to verify the authenticity of an executable code.

EV certificates are mainly intended for:

- Identification of the legal entity that controls a website: Reasonable assurance is given to the Internet browser user that the access to the website visited by it is controlled by a specific legal entity identified by an EV certificate wherein the following attributes have been verified: name, business address, jurisdiction of incorporation or registration, registration number or other unambiguous information; and
- Enabling encrypted communication with a website: Facilitating the exchange of encryption keys to enable encrypted communication of data over the Internet between the Internet browser user and the website.

The intended purpose of EV certificates has also helped establish the legitimacy of the business claiming to operate a website or distribute an executable code, and it further provides a vehicle that can be used to help solve issues related to phishing, malware, and other forms of online identity fraud. Providing a more reliable identity certified by a third party (Evrotrust) and

address information about the business, EV certificates:

- hinder phishing and other online attacks aimed at identity fraud;
- support companies that may be subject to phishing attacks or online identity fraud by providing them with a tool to better identify users;
- assist law enforcement organizations in their investigations of phishing and other online identity fraud cases, including, where appropriate, ensuring contacts with, investigation of or legal action against the subject.

EV certificates are solely focused on the identity of the subject named in the certificate and not on its behavior. As such, an EV certificate is not intended to provide any warranties or otherwise represent or warrant that:

- the subject named in the EV certificate is actively involved in doing business;
- the subject named in the EV certificate complies with the applicable laws;
- the subject named in the EV certificate is reliable, honest or reputable in its business transactions; or
- it is "safe" to do business with the subject named in the EV certificate.

1.4.2 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.

1.4.3 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, 1766

Business center MM, floor 5, Bul. Okolovrasten pat 251G

telephone, Fax: + 359 2 448 58 58

email: office@evrotrust.com

1.5.3 POLICY AND PRACTICE MANAGEMENT

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 on the Evrotrust website and are available to users, relying parties and all interested 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.

1.5.4.1 PROCEDURES FOR APPROVAL OF THE PRACTICE UPON PROVISION OF EV CERTIFICATES

Evrotrust develops, implements, applies, displays in a prominent place on its website and periodically updates a practice, policy and procedures for the issuance of EV certificates. Evrotrust applies the Browser Forum requirements and reviews them regularly. Evrotrust applies in its activities the requirements of the current WebTrust program for the CA, the current WebTrust program for EV, ETSI TS 102 042 for EVCP, or ETSI EN 319 411-1 for the EVCP policy.

Item 1.3.1 of this document describes the certification hierarchy of the Evrotrust and it allows for all used certificates to be traced up to their roots and which EV certificates depend on, as evidence of the authenticity of those EV certificates.

The management of Evrotrust is committed to following the Browser Forum recommendations. Evrotrust publicly announces in its Policy and Practice that it applies those requirements and adheres to the latest published version of the documents. Evrotrust applies the requirements of the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at <http://www.cabforum.org>. In the event of any inconsistency between this document and the Browser Forum recommendations, the latter shall prevail. Furthermore, Evrotrust incorporates (either directly or by reference) the applicable requirements in all contracts with subordinate CA, RA and subcontractors (if any) which are related to the issuance or maintenance of EV certificates. Evrotrust requires compliance with the said conditions.

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;

Repository - Database with Information available to Users and Relying Parties

Certification Authorization Authority (CAA) - In accordance with RFC 8659 (<http://tools.ietf.org/html/rfc8659>): “The Authorization Authority (CAA) enables the DNS domain name holder to indicate one or more certification authorities (CAs) to issue certificates for that domain name. CAA resource records allow a public CA to apply additional controls to reduce the risk of inadvertent certification.”

Applicant - The natural person or legal entity applying for (or requesting the renewal of) a certificate. After the issuance of the certificate, the applicant will be referred to as a user. For certificates issued for devices, the applicant is the subject that controls or manages the device referred to in the certificate, even if the device sends the actual certificate application.

Applicant's representative: A natural person, may be a sponsor, who is either a person hired by the applicant or an authorized agent who has the express power to represent the applicant:

- a) signing and representing, or approving the certificate request/application on behalf of the applicant and/or
- b) signing and representing the user contract (agreement) on behalf of the applicant and/or
- c) acknowledging the General Terms and Conditions on behalf of the applicant, where the applicant is an affiliate of a Certification Authority or is a Certification Authority itself.

Application Software Provider - A provider of Internet browser software or other

application software to the relying party that displays or uses certificates and incorporates certificates from the certification chain to its base certificate.

Letter of attestation - A letter certifying that the information about the subject is correct, written by an accountant, attorney-at-law, civil servant or other reliable third party who is normally relied upon for such information.

Authorization Domain Name - The domain name used to obtain permission to issue a certificate for an FQDN. Evrotrust may use a FQDN returned by a DNS CNAME reference as an FQDN for domain verification purposes. If the FQDN contains a wildcard, then Evrotrust removes all wildcards from the leftmost part of the requested FQDN. Evrotrust can remove zero or more characters from left to right until it encounters a base domain name and can use any of the intermediate values for domain verification purposes.

Authorized Ports - Any of the following ports: 80 (http), 443 (https), 25 (smtp), and 22 (ssh).

Base Domain Name - The part of the FQDN name applied for, which is the first part of the domain name (e.g. "example.co.uk" or "example.com"). For FQDNs where the rightmost part of the domain name is gTLD having ICANN specification 13 in its registry agreement, the gTLD itself can be used as the base domain name.

Cross Certificate - A certificate used to establish a trust relationship between two Root CAs.

Delegated Third Party - A natural person or legal entity authorized by Evrotrust, and whose activities do not fall within the scope of the relevant Evrotrust audits, to support the certificate management process by fulfilling or meeting one or more of the requirements of Evrotrust.

Domain Authorization Document - Documentation provided by or to Evrotrust for communication with the Domain Name Registrar, or a person/entity listed in WHOIS as a Domain Name Registrant (including any private, anonymous or proxy registration service), certifying the applicant's right to request a certificate for a specific Domain Namespace.

Domain Contact - The Domain Name Registrant, technical contact, or administrative contact (or ccTLD equivalent) as listed in the WHOIS record of the base domain name or DNS SOA record, or received through direct contact with the Domain Name Registrar.

Domain Name - The label assigned to a node in the Domain Name System.

Domain Namespace - The pool of all potential domain names that are subordinate to a node in the domain name system.

Domain Name Registrant - Sometimes referred to as the "owner" of a domain name, but more properly a natural person or legal entity who is referred to as a "registrant" by WHOIS or a domain name registrar who controls how the domain name is used.

Domain Name Registrar - A natural person or legal entity registering domain names under the auspices of or in agreement with:

- a) the Internet Corporation for Assigned Names and Numbers (ICANN),
- b) a national domain name authority/register, or
- c) a network.

Enterprise RA - An officer or agent of a non-Eurotrust organization that authorizes the issuance of certificates to that organization.

Fully-Qualified Domain Name - A Domain Name that includes the labels of all good nodes in the Domain Name System.

Governmental institution - A governmental legal entity, agency, department, ministry, branch or similar unit of the government of a country or political subdivision in such country (such as a state, province, city, county, etc.).

High Risk Certificate Request - Request for Eurotrust to implement additional controls, through the application of internal procedures which may include names with a higher risk of phishing or other fraudulent use, names contained in previously rejected certificate applications

or revoked certificates, names listed in the Miller Smiles Phishing List or in the Google Safe Browsing List, or names identified by Evrotrust using its own risk reduction criteria.

Internal Name - A string of characters (not IP addresses) in the common name or certificate subject field that cannot be verified as globally unique in the public DNS at the time the certificate is issued since it does not end with a Top Level Domain registered in IANA's Root Zone Database.

IP address: A 32-bit or 128-bit label assigned to a device that uses an Internet communication protocol.

IP Address Contact - The natural person registered with the IP Address Registration Authority who has the right to control how one or more IP addresses are used.

IP Address Registration Authority - Internet Assigned Numbers Authority (IANA) or Regional Internet Register (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Compromised key - a private key is compromised if its value has been disclosed to an unauthorized person and the latter had access to it.

Random value: A value designated for the applicant by Evrotrust that shows at least 112 bits of entropy (a physical quantity which is a measure of the disorder of thermodynamic systems).

Registered Domain Name - A domain name that is registered with the Domain Name Registrar.

Registration Authority (RA) - Any legal entity that is responsible for the identification and certification of certificate subjects, but is not a Certification Authority (CA) and therefore does not sign or issue certificates. The RA may assist in the process of applying for or revoking a certificate. The RA is part of Evrotrust.

Reliable Data Source: An identification document or data source used to verify the information about the identity of a subject that is generally recognized by commercial enterprises

and governments as being reliable and that has been created by a third party.

Reliable Method of Communication - A method of communication, such as a postal/courier delivery address, telephone number or e-mail address, which has been verified using a source other than the applicant's representative.

Relying Party: Any natural person or legal entity relying on a valid certificate. An application software provider shall not be considered a relying party where the software distributed by such provider simply displays information related to the certificate.

Subject - The natural person, device, system, unit or legal entity identified in the certificate as a subject. The subject is either the user (Subscriber) or a device under the user's control.

Subject Identity Information - Information that identifies the subject referred to in the certificate. Subject identity information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA - A certification authority (if any) whose certificate has been signed by the base CA of Evrotrust.

User (Subscriber) - A natural person or legal entity who has been issued a certificate and who is legally bound by a user contract or General Terms and Conditions.

User Contract - An agreement between Evrotrust and the applicant/user that sets out the rights and responsibilities of the parties.

Subsidiary - A company that is controlled by a parent company.

General Terms and Conditions - Provisions on the storage and use of certificates issued in accordance with the requirements of this document.

Valid Certificate - A certificate that has passed through the validation procedure referred to

in RFC 5280.

WHOIS - Information directly retrieved from the Domain Name Registrar or the registry operator through the protocol defined in RFC 3912, the registry data access protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate - A certificate containing an asterisk (*) in the leftmost position of any of the contained Subject Fully-Qualified Domain Names.

Wildcard Domain Name - A domain name consisting of a single asterisk followed by a single dot sign ("*.") followed by a Fully-Qualified Domain Name.

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;

PSD2 (Payment Services Directive 2) - The Revised Payment Services Directive; Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

PSP - Payment Service Provider

RA - Registration Authority;

SSL - Secure Socket Layer;

OCSP - Online Certificate Status Protocol;

TSP - Trust Service Provider.

AICPA - American Institute of Certified Public Accountants

ADN - Authorization Domain Name

CAA - Certification Authority Authorization

ccTLD - Country Code Top-Level Domain

CICA - Canadian Institute of Chartered Accountants

DBA - Doing Business As

DNS - Domain Name System

FQDN - Fully Qualified Domain Name

gTLDs - Generic Top-Level Domains

IANA - Internet Assigned Numbers Authority

ICANN - Internet Corporation for Assigned Names and Numbers

SSL - Secure Sockets Layer

TLS - Transport Layer Security

2 RESPONSIBILITY FOR PUBLISHING AND THE REPOSITORY

2.1 REPOSITORY

Evrotrust maintains a repository in which 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" are located. Evrotrust manages and controls the company's website where it publishing all current versions of electronic documents and provides secure and continuous access to them by stakeholders. The certificates register is a database in which are published all the issued Evrotrust certificates, which are used during its activity, user certificates and certificate revocation lists. 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).

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.

Evrotrust publicly discloses its "Certificate Policy for Qualified Certification Services for Website Authentication" and "Certification Practice Statement for Qualified Trust Services" through appropriate and easily accessible online tools that are available 24x7. Evrotrust publicly discloses its business practices to the extent required by the audit scheme under Regulation (EU) No. 910/2014.

The Policy and Practice are structured in accordance with RFC 3647. The Policy sets out the requirements for the use of domain names and for the processing of CAA records. This document sets out the set of domain names of the issuer recognized by the Certification Authority (CA) in the CAA "issue" or "issuewild" records as authorized for issuance. The Policy is publicly accessible and available to all interested parties in its latest up-to-date version.

Evrotrust registers all actions taken in the processing of information for the issuance of certificates, if any, in accordance with established procedures. All requirements fulfilled by Evrotrust when providing the service are described in this document. Evrotrust fulfills the requirements published at <http://www.cabforum.org> for the issuance and management of publicly trusted certificates. In the event of any inconsistency between this document and the Browser Forum requirements, the Browser Forum requirements shall prevail.

Evrotrust has in place test web pages that allow application software providers to test their software with their user (Subscriber) certificates which link to each publicly trusted base (Root) certificate. As a minimum, Evrotrust has individual web pages using user certificates that can be valid, suspended or terminated.

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 the 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, 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 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 TYPES OF NAMES

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

3.2 NECESSITY OF MEANINGFUL NAMES

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

3.3 ANONYMITY OR PSEUDONYMS OF USERS

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

3.4 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.

The name of the subject used in the certificate will never be used for (redirected to) another subject, unless the user provides evidence of lawful possession of the name.

3.5 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".

3.6 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.

3.7 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.

3.8 RECOGNITION, CERTIFICATION OF AUTHENTICATION AND ROLE OF THE TRADEMARK. DISPUTE SETTLEMENT PROCEDURE.

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

4 INITIAL REGISTRATION AND IDENTIFICATION/ESTABLISHMENT OF IDENTITY

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

An application for the issuance of a certificate may include all the factual information about the applicant that is included in the certificate, as well as additional information necessary for the purpose of complying with the requirements of the Evrotrust Policy and Practice. In cases where the certificate application does not contain all the necessary information about the applicant, Evrotrust will receive the remaining information either from the applicant or from a reliable, independent data source, after which the applicant shall confirm such information. Evrotrust follows an internal procedure to verify all data. Applicant information shall include, but shall not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the certificate's subjectAltName extension. Evrotrust may re-use previous verifications, provided that it has received the data or documents from a reliable source or has completed the verification itself no more than 398 days prior to the issuance of the certificate. Existing evidence may be re-used to verify identity depending on the applicable legislation and in consideration of whether

the evidence remains valid given the elapsed time. Evrotrust develops, maintains and implements documented procedures that identify and require additional activity to verify applications for high-risk certificates prior to the approval of the certificate itself. If a delegated third party (if any) is performing any of the Evrotrust's obligations, Evrotrust will verify that the process used by such third party to identify and further verify high-risk certificate applications provides at least the same level of security as Evrotrust's own processes.

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.

4.1 VERIFICATION OF PRIVATE KEY POSSESSION

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

4.2 ORGANIZATION AND DOMAIN IDENTITY VERIFICATION

Before issuing a certificate, a verification is made on the applicant's legal existence and identity. If the applicant requests a certificate containing information on the subject's identity, consisting only of the countryName field, then Evrotrust will verify the country associated with the subject by using an approved verification procedure. If the applicant requests a certificate that will contain, in addition to the countryName field, also other information about the subject's identity, then Evrotrust will verify the applicant's identity and the authenticity of the certificate request made by the applicant's representative by using a verification procedure. Evrotrust verifies every document which the identity verification is referred to for any alteration or falsification.

Evrotrust determines how it will perform the organization and domain identity verification.

4.2.1 IDENTITY VERIFICATION

If the subject's identity information is to include the name or address of the organization, Evrotrust verifies the identity and address of the organization and, more specifically, that the address indicated is the address of the applicant's existence or place of business. Evrotrust verifies the applicant's identity and address by using documentation provided by or through

communication in at least one of the following ways:

- Government agency based in the applicant's jurisdiction of lawful establishment, existence or recognition;
- Third party database which is periodically updated and is considered a reliable data source;
- On-site visit by a Evrotrust representative or a third party acting as a Evrotrust agent; or
- A letter of attestation.

Evrotrust may use the same documentation or communication as described in the above 4 (four) points in order to verify both the identity and the address of the applicant. Alternatively, Evrotrust may verify the applicant's address (but not the applicant's identity) by using a utility bill, bank statement, credit card statement, issued state tax document or any other form of identification that Evrotrust deems reliable.

4.2.2 TRADE NAME/DBA

If the subject's identity information is to include a DBA or a trade name, Evrotrust verifies the applicant's right to use a DBA/trade name by using at least one of the following methods of verification:

- Documentation provided by or communication with a government agency based in the applicant's jurisdiction of lawful establishment, existence or recognition;
- Reliable data source;
- Communication with a government agency responsible for the management of such DBAs or trade names;
- Letter of attestation accompanied by documentary support; or
- Utility bill, bank statement, credit card statement, issued state tax document or any other form of identification that Evrotrust deems reliable.

4.2.3 COUNTRY VERIFICATION

If the subject: countryName is present, then the Evrotrust verifies the country associated with the subject by using one of the following methods:

- a) assignment of a range of IP addresses by country for any of them:
 - The IP address of the website as specified by the DNS record for the website, or
 - The IP address of the applicant;

- b) ccTLD
- c) the requested domain name;
- d) information provided by the Domain Name Registrar; or
- e) another method of identification described in this document.

Evrotrust shall implement a proxy server screening process to prevent the deciphering of IP addresses assigned in countries other than the applicant's location.

4.2.4 DOMAIN CERTIFICATION OR CONTROL VERIFICATION

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.

This Policy sets out the permitted processes and procedures for validating the applicant's ownership or control of the domain. Prior to issuing a certificate, Evrotrust shall confirm each Fully-Qualified Domain Name (FQDN) listed in the certificate as follows:

1. Where the FQDN **does not contain** "onion" as the rightmost label, Evrotrust validates the FQDN using at least one of the methods referred to below;
2. Where the FQDN **contains** "onion" as the rightmost label, Evrotrust validates the FQDN in accordance with the requirements for the issuance of .onion Domain Names certificates. Eligible verification procedures are followed for inclusion of one or more RFC 7686 ".onion" Domain Names for special use in the certificates. The verifications of the applicant completed by Evrotrust may be valid for the issuance of multiple certificates over time. In any case, the validation must have started within the period specified in the relevant requirement prior to the issuance of the certificate. For domain validation purposes, the term "applicant" shall include the applicant's parent company, subsidiary or affiliate. Evrotrust maintains a record of which domain verification method was used, including the corresponding EV Guidelines version number used to validate each domain. FQDNs can be listed in the user (Subscriber) certificate using dNSNames in the subjectAltName extension or in subordinate CA certificates via dNSNames in the

permittedSubtree within the Name Constraints extension.

4.2.4.1 SENDING E-MAIL, FAX, SMS OR MAIL TO A DOMAIN CONTACT

The method confirms the applicant's control over the FQDN by sending a random value by e-mail, fax, SMS or mail and then receiving a confirmatory response using the random value. The random value is sent to an e-mail address, fax/SMS number, or mail identified as Domain Contact. Each e-mail, fax, SMS or mail can confirm the control of multiple domains. Evrotrust may send an e-mail, fax, SMS or mail to more than one recipient, provided that each recipient has been identified by the Domain Name Registrar as representing a Domain Name Registrar for each FQDN that is verified by e-mail, fax, SMS or mail. The random value must be unique for each e-mail, fax, SMS or mail. Evrotrust may re-send the e-mail, fax, SMS or mail in full, including the re-use of the random value, provided that all content and recipient(s) of the communication remain unchanged. The random value remains valid for use in a confirmatory response for no more than 30 days from its creation. Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.2 CREATING AN E-MAIL FOR A DOMAIN CONTACT

Confirmation of the applicant's control over the FQDN can be made by:

- sending an e-mail to one or more addresses created using "admin", "administrator", "webmaster", "hostmaster" or "postmaster" as a local part, followed by at-sign ("@"), followed by Authorization Domain Name;
- including a random value in the e-mail;
- receiving a confirmatory response using the random value.

Each e-mail confirms control of multiple FQDNs, provided that the Authorization Domain Name used in the e-mail is the Authorization Domain Name for each confirmed FQDN. The random value must be unique in each e-mail. An e-mail may be forwarded in its entirety, including the re-use of the random value, provided that all its content and the recipient remain unchanged. The random value shall remain valid for use in the confirmatory response for no more than 30 days from its creation. Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.3 AGREED CHANGE OF WEBSITE

Confirmation of the applicant's control over the FQDN by confirming one of the following options in the "/.wellknown/ pki-validation" directory or another path registered in the IANA for the purposes of Domain Validation of a Domain Name Authorization accessed by Evrotrust via HTTP/HTTPS through an authorized port:

- The presence of mandatory website content contained in a file's content. All mandatory website content may not appear in the request used to retrieve the file or webpage, or
- The presence of a Request Token or Random Value contained in a file's content, where the Request Token or Random Value may not be displayed in the request. If a random value is used, Evrotrust provides such value unique to the certificate application and will not use the value for a period longer than:

- 30 days, or
- if the applicant has applied for a certificate, for the period of time allowed

for re-use of the validated information related to the certificate.

Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.4 CHANGE OF DNS

This is a method of confirming the applicant's control over the FQDN by confirming the presence of a Random Value or Request Token in the DNS CNAME, TXT or CAA record for:

- Authorization Domain Name, or
- Authorization Domain Name, which has a label prefix starting with an underscore.

If a random value is used, Evrotrust provides that value unique to the certificate application and will not use the random value for a period longer than:

- 30 days, or
- the period allowed for re-use of the validated information related to the certificate.

Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.5 IP ADDRESS

A method of confirming the applicant's control over the FQDN by confirming that the applicant controls the IP address returned by a DNS reference for A or AAAA records for the FQDN. Once the FQDN has been validated using this method, Evrotrust may **not** issue certificates for other FQDNs ending with all labels of the validated FQDN, unless Evrotrust performs a separate verification of that FQDN using an authorized method. This method is **not** suitable for validating Wildcard Domain Names.

4.2.4.6 VERIFICATION OF THE APPLICANT AS A DOMAIN CONTACT

A method of confirming the applicant's control over the FQDN by validating the applicant with a Domain Contact. This method can only be used if Evrotrust is also a Domain Name Registrar or an Affiliate of the Base Domain Name Registrar. Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.7 SENDING E-MAIL TO A DNS CAA CONTACT

A method of confirming the applicant's control over the FQDN by sending a random value by e-mail and then receiving a confirmatory response using such random value. The random value shall be sent to the DNS CAA e-mail contact. The relevant CAA Resource Record Set shall be found using the search algorithm defined in RFC 8659, Section 3.

Each e-mail can confirm control of multiple FQDNs, provided that each e-mail address is a DNS CAA e-mail contact for each authorization domain name. The same e-mail can be sent to multiple recipients, as long as all recipients are DNS CAA e-mail contacts for each verified Authorization Domain Name.

The random value must be unique in each e-mail. The e-mail may be forwarded in its entirety, including the re-use of the random value, provided that all its content and recipient(s) remain unchanged. The random value shall remain valid for use in the confirmatory response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.8 SENDING AN E-MAIL TO A DNS TXT CONTACT

A method of confirming the applicant's control over the FQDN by sending a random value by e-mail and then receiving a confirmatory response using such random value. The random value is sent to the DNS TXT Record Email Contact of the Authorization Domain Name selected for FQDN verification.

Each e-mail can confirm control of multiple FQDNs, provided that such e-mail address is a DNS TXT Record Email Contact for each Authorization Domain Name being verified. The same e-mail can be sent to multiple recipients, as long as all recipients are DNS TXT Record Email Contacts for each validated Authorization Domain Name.

The random value shall be unique in each e-mail. The e-mail may be forwarded in its entirety, including the re-use of the random value, provided that all its content and recipient(s) remain unchanged. The random value shall remain valid for use in a confirmatory response for no more than 30 days from its creation. Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.9 TELEPHONE CONTACT WITH A DOMAIN CONTACT

A method of confirming the applicant's control over the FQDN after calling the Domain Contact telephone number and receiving a confirmatory response for the ADN verification. Each telephone call can confirm the control of multiple ADNs, provided that the same domain contact telephone number is indicated for each ADN being verified and a confirmatory response is provided for each ADN.

In case another Domain Contact is accessed, Evrotrust may request to be transferred to Domain Contact. In case of access to voicemail, Evrotrust may let the random value and the ADN(s) to be confirmed. The random value shall be returned to Evrotrust to approve the request.

The random value shall remain valid for use in a confirmatory response for no more than 30 days from its creation. Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.10 TELEPHONE CONTACT WITH A DNS TXT RECORD PHONE CONTACT

A method of confirming the applicant's control over the FQDN after calling the DNS TXT

Record Phone Contact telephone number and receiving a confirmatory response for the ADN verification. Each telephone call can confirm control of multiple ADNs, provided that the same DNS TXT Record Phone Contact telephone number is indicated for each ADN being verified and a confirmatory response is provided for each ADN.

Evrotrust cannot be knowingly transferred or request to be transferred, since this telephone number is specifically provided for domain validation purposes.

In case of access to voicemail, Evrotrust may let the random value and the ADN(s) to be confirmed. The random value shall be returned to Evrotrust to approve the request. The random value shall remain valid for use in a confirmatory response for no more than 30 days from its creation. Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.11 TELEPHONE CONTACT WITH A DNS CAA PHONE CONTACT

A method of confirming the applicant's control over the FQDN after calling the DNS CAA Phone Contact telephone number and receiving a confirmatory response for the ADN verification. Each telephone call can confirm control of multiple ADNs, provided that the same DNS CAA contact telephone number is indicated for each ADN being verified and a confirmatory response is provided for each ADN. The relevant CAA Resource Record Set must be found using the search algorithm defined in RFC 8659, Section 3.

Evrotrust shall not be transferred or request to be transferred, since this telephone number is explicitly provided for domain validation purposes. In case of access to voicemail, Evrotrust may let the random value and the ADN(s) to be confirmed. The random value shall be returned to Evrotrust to approve the request. The random value shall remain valid for use in a confirmatory response for no more than 30 days from its creation. Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.12 AGREED CHANGE OF V2 WEBSITE

A method of confirming the applicant's control over the FQDN by verification so that the Request Token or Random Value is contained in a file's content: 1. The entire request token or random value shall not be displayed in the request used to retrieve the file; and 2. Evrotrust shall

receive a successful HTTP response from the request (meaning that a 2xx HTTP status code shall be received). The file containing a request token or random value: 1. shall be located in the Authorization Domain Name; 2. shall be located in the "/.well-known/pki-validation" directory; 3. shall be retrieved via "http" or "https"; and 4. shall be accessed through an authorized port.

In case Evrotrust applies a method with redirections, the following shall apply: 1. The redirections are initiated at the HTTP protocol level (e.g. using a 3xx status code); 2. The redirections are obtained as a result of an HTTP status code within the 3xx status code redirection class as defined in RFC 7231, Section 6.4; 3. The redirections are to URL type resources or via "http" or "https" protocols; and 4. The redirections are to URLs of resources accessed through authorized ports.

If a random value is used, then: 1. Evrotrust provides such random value unique to the certificate application; 2. The random value shall remain valid for use in a confirmatory response for no more than 30 days from its creation. Once the FQDN has been validated using this method, Evrotrust may issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.13 AGREED CHANGE OF WEBSITE - ACME

A method of confirming the applicant's control over the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555. The following additional requirements shall apply to this method: Evrotrust shall receive a successful HTTP response from the request (meaning that it must receive a 2xx HTTP status code); and the Token (as defined in RFC 8555, Section 8.3) shall not be used for more than 30 days from its creation.

If Evrotrust applies redirections: 1. The redirections must be initiated at the HTTP protocol level (e.g. using a 3xx status code); 2. The redirections must be the result of an HTTP status code within the 3xx class of redirecting status codes as defined in RFC 7231, Section 6.4; 3. The redirections must be to URLs or via "http" or "https"; and 4. The redirections must be to URLs of resources accessed through authorized ports.

Once the FQDN has been validated using this method, Evrotrust may also issue certificates for other FQDNs ending with all labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

4.2.4.14 TLS USE OF ALPN

A method of confirming the applicant's control over the FQDN by negotiating a new application layer protocol using TLS Application-Layer Protocol Negotiation (ALPN) [RFC7301] as defined in RFC 8737. The token shall not be used for more than 30 days from its creation. Once the FQDN has been validated using this method, Evrotrust may not issue certificates for other FQDNs ending with all labels of the validated FQDN, unless Evrotrust performs a separate verification for that FQDN using an authorized method. This method is not suitable for validating Wildcard Domain Names.

4.2.5 CERTIFICATION FOR IP ADDRESS

This document defines the permitted processes and procedures for validating the applicant's ownership or control of the IP address indicated in the certificate. Evrotrust shall confirm, before issuing the certificate, each IP address indicated therein, using one of the methods listed below. Completed verifications allow for the issuance of multiple certificates over a period of time. In any case, the validation must have started before the issuance of the certificate. For the purposes of IP address validation, the term "applicant" shall include the applicant's parent company, subsidiary or affiliate. Evrotrust keeps a record of which IP address validation method, including the corresponding BR (CA/Browser Forum) version number, was used to validate each IP address.

The verified IP addresses may be listed in the user (Subscriber) certificates or in the sub-certificates of Evrotrust via `iPAddress` in `permittedSubtrees` within the Name Constraints extension. Evrotrust shall not be under the obligation to verify any IP addresses listed in Subordinate CA Certificates via `iPAddress` in `excludedSubtrees` within the Name Constraints extension before their inclusion in a Subordinate CA Certificate.

4.2.5.1 AGREED CHANGE OF WEBSITE

A method of confirming the applicant's control over the IP address applied for, by verifying the presence of a Request Token or Random Value contained in the content of a file or web page in the form of a meta tag in the `"/.well-known/pki-validation"` directory or another path registered in the IANA for the purpose of validating the control of IP addresses, to an IP address that is accessible by Evrotrust via HTTP/HTTPS through an authorized port. The request token or random value shall not be displayed in the request.

If a random value is used, Evrotrust provides such random value unique to the certificate application and will not use it for a period longer than 30 days or, where the applicant has submitted a certificate application stating an allowed period for re-use of validated information, within such period.

4.2.5.2 SENDING E-MAIL, FAX, SMS OR MAIL TO AN IP ADDRESS CONTACT

A method of verifying the applicant's control over an IP address by sending a random value by e-mail, fax, SMS or mail and then receiving a confirmatory response using such random value. The random value is sent to an e-mail address, fax/SMS number, or mail address identified as an IP Address Contact.

Each e-mail, fax, SMS or mail can confirm control of multiple IP addresses. Evrotrust may send an e-mail, fax, SMS or mail with a unique random value to more than one recipient, provided that each recipient has been identified by the IP Address Registration Authority as representing an IP Address Contact for each IP address being verified. Evrotrust may re-send an e-mail, fax, SMS or mail and re-use the random value, provided that all content and communication remain unchanged. The random value shall remain valid for use in the confirmatory response for no more than 30 days from its creation.

4.2.5.3 SEARCH FOR A REVERSE ADDRESS

A method of confirming the applicant's control over an IP address by obtaining a Domain Name associated with the IP address through reverse-IP search of an IP address and subsequent confirmation of the control over the FQDN.

4.2.5.4 TELEPHONE CONTACT WITH AN IP ADDRESS CONTACT

A method of verifying the applicant's control over the IP address by calling the IP Address Contact telephone number and receiving a response confirming the applicant's request for the IP address validation. Evrotrust shall place the call on a telephone number identified by the IP Address Registration Authority as the IP Address Contact. Each telephone call shall be made to a single number. In the event that someone other than the IP Address Contact is accessed, Evrotrust may request to be transferred to the IP Address Contact. In case of access to a voicemail, Evrotrust may let the random value and the IP addresses to be confirmed. The random value shall be returned to Evrotrust in order for the request to be approved. The random value shall remain valid

for use for no more than 30 days from its creation.

4.2.5.5 ACME "HTTP-01" METHOD FOR IP ADDRESSES

A method of confirming the applicant's control over the IP address by performing the procedure documented for the use of the "http-01" challenge in project 04 of the "ACME IP Identifier Validation Extension" accessible at <https://tools.ietf.org/html/draft-ietf-acme-ip-04> # section-4.

4.2.5.6 ACME METHOD "TLS-ALPN-01" FOR IP ADDRESSES

A method of confirming the applicant's control over the IP address by performing the procedure documented for the use of the "tls-alpn-01" challenge in project 04 of the "ACME IP Identifier Validation Extension" accessible at <https://tools.ietf.org/html/draft-ietf-acme-ip-04> # section-4.

4.2.5.7 WILDCARD DOMAIN VERIFICATION

Before issuing a wildcard (*) certificate in a CN or subjectAltName of the DNS-ID type, Evrotrust establishes and documents a procedure that determines whether the wildcard appears in the first position of the label left from the "register" - controlled "label or public suffix" (e.g: "*.com" or "*.co.uk" as described in RFC 6454).

If the wildcard appears on the label immediately on the left, Evrotrust refuses the issuance, unless the applicant proves its legal control over the entire Domain Namespace. (e.g. "*.co.uk" or "*.local" are not issued, but "*.example.com" may be issued).

The definition of what is "registry-controlled" in relation to the registered part of the Country Code Top-Level Domain Namespace is not standardized at the time of entry and is not the property of the DNS itself. The current best practice comes down to enabling reference to the Public Suffix List (PSL) and obtaining a relevant up-to-date copy.

If the PSL is used, Evrotrust only refers to the ICANN DOMAINS section and not the PRIVATE DOMAINS section. The PSL is updated regularly to include new gTLDs delegated by ICANN that are listed in the ICANN DOMAINS. Evrotrust does not issue a Wildcard Certificate to the Registrant of the entire gTLD, provided that the control of namespace by name is demonstrated in one way only.

4.2.6 ACCURACY OF THE DATA SOURCE

Before using any source as a reliable data source, Evrotrust shall assess the source in terms of its reliability, accuracy and resistance to alteration or falsification. In its assessment, Evrotrust will take into account the following:

- a) The age of the information provided;
- b) The frequency of updates to the source of information;
- c) The data provider and the purpose of the data collection;
- d) The public access to data availability; and
- e) The relative difficulty to falsify or alter the data.

The databases kept by Evrotrust or its affiliated companies are **not** a reliable data source if the main purpose of the database is to collect information in order to fulfil the validation requirements.

4.2.7 CAA RECORDS

As part of the certification process, Evrotrust checks for CAA records and follows the instructions for processing each `dNSName` in the `subjectAltName` extension of the certificate to be issued. If Evrotrust issues a certificate, it shall do so within the TTL of the CAA record or within 8 hours, whichever of the two is longer. This requirement shall not prevent Evrotrust from verifying the CAA records at any other time. As CAA records, Evrotrust processes the `issue`, `issuewild` and `iodef` property tags, although no action is required on the content of the `iodef` property tag. Additional property tags may be maintained, but they shall not conflict with or replace the mandatory property tags. Evrotrust takes into account the critical flag and does not issue certificates if it encounters an unrecognized property with that flag. Evrotrust may treat a non-empty CAA resource record set that does not contain issue property tags as an issue authorization, provided that the records in the CAA resource set do not prohibit the issue.

Evrotrust allows exceptions in the following cases:

- CAA verification is not mandatory for certificates for which a Certificate Transparency pre-certificate has been created and it has been entered in at least two public registration files for which CAA has been verified;
- CAA verification is not mandatory for certificates issued by the Technically Constrained Subordinate CA Certificate, where the absence of CAA verification is an explicitly agreed provision in the contract with the applicant;

➤ CAA verification is not mandatory if Evrotrust or an Affiliate of Evrotrust is a DNS operator of the domain DNS.

Evrotrust may issue certificates when the search for a record is unsuccessful, if:

- the damage is beyond the Evrotrust infrastructure;
- the search has been attempted at least once; and
- the domain zone does not have a DNSSEC validation chain to the ICANN root.

Evrotrust documents in detail potential issues that were hindered by the CAA record in order to notify the CAB forum accordingly. Evrotrust sends the reports of those issue requests to the described contacts listed in the CAA iodef record(s), if such are present. Evrotrust does not support URL schemes in an iodef record other than mailto: or https:.

4.3 CERTIFICATION OF THE IDENTITY OF A NATURAL PERSON

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

If the applicant (subject) is a natural person, then Evrotrust verifies:

- The full name (including surname and first name(s) corresponding to national identification practices),
- the applicant's address, and
- the authenticity of the certificate application.

Evrotrust may, where necessary, verify other attributes of the person, such as date and place of birth.

Evrotrust verifies the applicant's name using a legible copy that clearly shows the applicant's face in at least one currently valid national photo ID (passport, driving license, military ID, national ID or equivalent). Evrotrust checks the copy for any indications of alteration or falsification. Evrotrust verifies the applicant's address using an identification form that Evrotrust deems reliable, such as a national identity document, a utility bill, a bank statement or a credit card. The Evrotrust verification may be based on the same state-issued identity document that was used to confirm the applicant's name. Evrotrust verifies the certificate application with the applicant using a reliable method of communication.

4.4 VERIFICATION OF THE POWER OF REPRESENTATION

If an applicant for a certificate containing the subject's identity information is an organization, Evrotrust shall use a reliable method of communication to verify the authenticity of the certificate application filed by the applicant's representative.

Evrotrust may use the sources listed in this document to verify the reliability of the method of communication. Provided that Evrotrust uses a reliable method of communication, the provider may establish the authenticity of the certificate application directly with the applicant's representative or with an authoritative source in the applicant's organization, such as a business or corporate office, human resources office, information technology office or another department that Evrotrust deems appropriate.

In addition, Evrotrust establishes a process that allows the applicant to identify the persons who may request certificates. If the applicant designates in writing the persons who may request a certificate, then it does not need to accept applications for certificates that are outside this list. Evrotrust will provide the applicant with a list of its authorized certificate applicants upon the applicant's confirmed written request.

4.5 SPECIAL ATTRIBUTES

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

4.6 UNCONFIRMED INFORMATION

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

4.7 INTEROPERABILITY CRITERIA

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 whatsoever and the quality of service should not be impaired

Evrotrust discloses all cross certificates that identify it as a subject, provided that Evrotrust has established or accepted the establishment of a trust relationship, i.e. it has issued a Cross

Certificate.

4.8 IDENTIFICATION AND IDENTITY ESTABLISHMENT UPON RENEWAL OF A QUALIFIED CERTIFICATE

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

4.9 IDENTIFICATION AND IDENTITY ESTABLISHMENT UPON SUSPENSION OF A QUALIFIED CERTIFICATE

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

4.10 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".

4.11 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".

5 REQUIREMENTS FOR REGISTRATION AND VERIFICATION OF AN APPLICANT FOR THE ISSUANCE OF EV CERTIFICATES

Evrotrust complies with the requirements of the current versions of CA/Browser Forum Version Guidelines for the Issuance And Management of Extended Validation Certificates and CA/Browser Forum Version Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates when registering, identifying and issuing EV certificates. Evrotrust issues EV certificates only to applicants who meet the requirements for a private organization, governmental body, business entity and non-profit organization.

Evrotrust determines by itself how it will perform the verification according to the requirements for registration and verification of an applicant for the issuance of EV certificates.

5.1 IDENTIFICATION AND ESTABLISHMENT OF IDENTITY

Before issuing an EV certificate, Evrotrust shall ensure that all factual information about the applicant to be included in the certificate, as well as the necessary additional information received from the applicant, complies with the legal requirements and the Evrotrust certification policy. In cases where additional information is received from a third party, a reliable independent data source, such information shall be confirmed by the applicant. Evrotrust follows an established procedure for verifying all data requested by the applicant to be included in the certificate.

The information about the applicant shall include, but shall not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the certificate's subjectAltName extension.

Evrotrust may use the documents and data provided by the applicant to verify the information about the certificates, or may re-use the previous verifications themselves, provided that it has received the data or documents from a reliable source, or has completed the verification itself no more than 398 days before issuance of the certificate. Evrotrust will not re-use data or documents used in the previous validation if they have been obtained for more than the maximum time allowed for re-use of such data or document before issuance of the certificate.

Evrotrust develops, keeps and applies documented procedures that identify and require additional action to verify applications for high-risk certificates prior to the approval of the certificate in order to ensure that such applications are properly verified in accordance with the regulatory requirements.

If an authorized third party is performing any of Evrotrust's identification obligations, Evrotrust shall ensure that the process of identification and additional verification of applications has at least the same level of security as its own processes.

5.2 GENERAL VERIFICATION REQUIREMENTS IN ACCORDANCE WITH CA/BROWSER FORUM

Evrotrust applies validation duty segregation procedures to ensure that no officer can severally validate and authorize the issuance of an EV certificate. Cross-correlation and due diligence may be performed by one officer of the Registration Authority who reviews and verifies all of the applicant's information and a second officer of the Registration Authority who validates and approves the issuance of an EV certificate. The validation control must be monitored.

The verification at initial registration aims to achieve the following:

- 1.** Verification of the existence and identification of the applicant's identity, including;
 - a)** Verification of the applicant's legal existence and identity;
 - b)** Verification of the applicant 's physical existence (business presence at a physical address); and
 - c)** Verification of the applicant's operational existence (business activity).
- 2.** Evrotrust certifies that the applicant is a registered holder or has exclusive control over the domain name(s) to be included in the EV certificate.
- 3.** Evrotrust verifies the reliable means of communication with the subject to be indicated in the certificate;
- 4.** Evrotrust verifies the authorization of the applicant for an EV certificate, including whether the certificate approver has signed or approved the application for an EV certificate.

5.2.1 OVERVIEW OF ELIGIBLE VERIFICATION METHODS

As a general rule, Evrotrust is responsible for taking all verification steps. The eligible verification methods, which usually include alternatives, are considered the minimum acceptable level of verification. In any case, however, Evrotrust shall be responsible for carrying out any additional verifications that may be necessary to fulfill the applicable verification requirement.

5.2.2 DISCLOSURE OF VERIFICATION SOURCES

Evrotrust provides publicly, through appropriate and easily accessible online means, the information verification requirements, such as the use of a Registry Agency or a Registration Agency. The information about the agency shall include, as a minimum, the following:

- Sufficient information for unambiguous identification in the Registry Agency or the Registration Agency (such as name, jurisdiction and website); and
- Value for each subject: jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1), jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2) and jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3) upon issuance of a certificate; and
- The eligible form or syntax of the registration numbers used by the Registry Agency or the Registration Agency; and
- Revision history, which includes a unique version number and publication date for

any supplementations, modifications and/or removals from this list.

Evrotrust has described the said information in this document.

5.3 VERIFICATION OF THE APPLICANT'S LEGAL EXISTENCE AND IDENTITY

5.3.1 VERIFICATION REQUIREMENTS

In order to verify the applicant's legal existence and identity, Evrotrust verifies:

5.3.1.1 IDENTIFICATION/ESTABLISHMENT OF THE IDENTITY OF A PRIVATE ORGANIZATION SUBJECT

- 1. Legal existence:** A verification is performed as to whether the applicant is a legally recognized entity existing and validly formed (e.g. registered) in a Registry Agency or a Registration Agency in the applicant's jurisdiction of incorporation or registration and is not listed in the Agency's registers as "inactive", "invalid", "non-current", or the like.
- 2. Name of the organization:** A verification is performed as to whether the official name of the applicant entered with the Agency in the applicant's jurisdiction of incorporation or registration coincides with the applicant's name in the EV certificate application.
- 3. Registration number:** Obtaining the specific registration number assigned to the applicant by the relevant agency in the applicant's jurisdiction of incorporation or registration. Where the Agency does not assign a registration number, Evrotrust will obtain the date of entry or registration of the applicant.
- 4. Registered agent:** Evrotrust takes the identity and address of the registered agent or the registered office of the applicant (as applicable in the applicant's jurisdiction of incorporation or registration).

5.3.1.2 ESTABLISHMENT OF THE IDENTITY OF GOVERNMENTAL SUBJECTS

In order to verify the applicant's legal existence and identity, Evrotrust verifies:

- 1. Legal existence:** A verification is performed as to whether the applicant is a legally recognized governmental body that exists in the political subdivision wherein such governmental body operates.
- 2. Name of the subject:** A verification is performed as to whether the official legal name of the applicant coincides with the name of the applicant in the EV certificate application.
- 3. Registration number:** Evrotrust looks for information about the date of incorporation,

registration or establishment of the applicant or the identifier of the legislative act that established the governmental body. In cases where such information is not available, Evrotrust, at its own discretion, will seek a way to indicate that the subject is a government institution.

5.3.1.3 ESTABLISHMENT OF THE IDENTITY OF BUSINESS SUBJECTS

In order to verify the applicant's legal existence and identity, Evrotrust verifies:

- 1. Legal existence:** Evrotrust verifies whether the applicant is engaged in business under the name indicated in the application.
- 2. Name of the organization:** A verification is performed as to whether the official legal name of the applicant recognized by the Registration Agency in the applicant's jurisdiction matches the name of the applicant given in the EV certificate application.
- 3. Registration number:** Evrotrust takes the necessary steps to obtain the specific unique registration number assigned to the applicant by the Registration Agency in the applicant's jurisdiction. Where the Registration Agency does not assign a registration number, Evrotrust will obtain the applicant's registration date.
- 4. Chief Natural Person (director, chief):** Evrotrust verifies the identity of the identified chief natural person.

5.3.1.4 ESTABLISHMENT OF THE IDENTITY OF NON-PROFIT SUBJECTS (INTERNATIONAL ORGANIZATIONS)

In order to verify the applicant's legal existence and identity, Evrotrust verifies:

- 1. Legal existence:** Evrotrust verifies whether the applicant is a legally recognized subject of the international organization.
- 2. Name of the subject:** A verification is performed as to whether the official legal name of the applicant coincides with the name of the applicant in the EV certificate application.
- 3. Registration number:** Evrotrust takes the necessary steps to obtain the date of establishment or the identifier of the legislative act that established the International Organization. In cases where such information is not available, Evrotrust will, at its own discretion, seek a way to indicate that the subject is an international organization.

5.3.2 ELIGIBLE VERIFICATION METHODS

Evrotrust permits the following verification methods:

5.3.2.1 PRIVATE ORGANIZATION SUBJECTS

The identity of private organization subjects is verified, either directly or indirectly, by documents obtained from the Registry or Registration Agency in the applicant's jurisdiction. Such verification may be performed by using a reliable governmental information source managed by or on behalf of the Registry or Registration Agency, or through direct contact with the Agency by post, e-mail, web address or telephone, for this purpose using an address or telephone number obtained directly from the reliable governmental information source or from a reliable independent source of information.

5.3.2.2 GOVERNMENT SUBJECTS

The required documents of government subjects are verified directly or are obtained from: a reliable governmental source in the political subdivision where such governmental body operates; a senior government agency in the same political subdivision as the applicant, or from a judge who is an active member of the state or local judiciary within the same political subdivision. Any information from a judge shall be verified in the same way as data obtained from an attorney-at-law. Such verification may be performed personally with the relevant governmental body or by post, e-mail, web address or telephone, using an address or telephone number obtained from a reliable independent source of information.

5.3.2.3 BUSINESS SUBJECTS

The verification of business subjects is performed directly or through the Registry Agency in the applicant's jurisdiction. Such verification may be performed through a reliable source of governmental information, a reliable governmental source of tax information, or through direct contact with the Registration Agency, either personally or by post, e-mail, web address or telephone, using an address or telephone number obtained directly from a reliable government source of information, reliable governmental source of tax information or Registration Agency, or from a reliable independent source of information. In addition, Evrotrust verifies the identity of the chief natural person (e.g. CEO) associated with the business subject.

5.3.2.4 CHIEF NATURAL PERSON

The establishment of the identity of the chief natural person associated with the business

subject is performed face to face. Evrotrust performs a face-to-face verification, but may also rely on a face-to-face validation of the chief person by the Registration Agency, provided that Evrotrust has assessed the face-to-face validation procedure.

1. Face-To-Face Verification: The face-to-face verification is performed in front of a Evrotrust officer, notary, attorney-at-law or financial authority (third party validator). The chief person(s) must submit documents for verification directly to the third party validator:

a) Personal statement including the following information:

- (1) Full name or names by which the person is known or has been known (including all other names used);
- (2) Address at the place of residence at which it may be located;
- (3) Date of birth; and
- (4) Confirmation that all the information contained in the certificate application is correct.

b) A current nationally recognized identity document that includes a photograph of the natural person and is signed by the natural person, such as:

- (1) Passport;
- (2) Driver's license;
- (3) ID card;
- (4) Weapon permit; or
- (5) Military ID document.

c) At least two pcs. of secondary documentary evidence, including the name of the natural person, for establishing the identity of the person, one of which being from a financial institution.

(1) The eligible documents from the financial institution include:

- i. Valid credit card;
- ii. Valid debit card from a regulated financial institution,
- iii. Mortgage statement from a recognizable lender issued less than six months ago,
- iv. Bank statement from a regulated financial institution issued less than six months ago.

(2) Eligible non-financial documents include:

- i. Latest original utility bills or evidence from the utility company confirming the arrangement to pay for the services at a fixed address. A mobile/cell phone bills

is not acceptable,

- ii. A copy of a lease payment statement, provided that such statement dates from the last six months,
- iii. Certified copy of a birth certificate,
- iv. Tax bill from the local government for the current year,
- v. Certified copy of a court order (for example, divorce certificate or adoption documents).

In cases where a third party carries out a face-to-face verification, the following documents shall be provided:

- a) a signed personal declaration and a nationally recognized identity document of the signatory; and
- b) verification of the original documents used for identification. The third party shall certify that the copy of the nationally recognized identity document with a photograph is complete, true and accurately reproduces the original.

2. Third party verification: Evrotrust verifies that the third party validator is a legally recognized notary, attorney-at-law or financial authority in the individual's jurisdiction and that the third party validator has actually performed the services and certified the verification with its signature.

3. Cross-checking of the information: Evrotrust shall receive a signed and valid personal statement and a valid personal identity document with a photograph. Evrotrust reviews the documentation to determine whether it is complete, compliant and identifies the natural person. Evrotrust relies on electronic copies of such documentation, provided that:

- a) Evrotrust can confirm their authenticity with the third party validator; and
- b) The electronic copies of such documents are recognized as legal substitutes for the originals under the national law.

5.3.2.5 NON-PROFIT (INTERNATIONAL ORGANIZATION) SUBJECTS

Evrotrust verifies:

- a) the instrument of incorporation establishing the international organization;

- b) Performs a verification through direct contact with the government of the country where Evrotrust conducts business. Such verification may be obtained from an appropriate government agency, from the legislative authorities of that country, or through verification of whether the government of the country has a mission to represent it in the international organization; or
- c) Directly from any current list of trusted subjects that may be kept by the CA/Browser Forum at www.cabforum.org.
- d) In cases where the international organization applying for an EV certificate is a body or agency - including a non-governmental organization, then Evrotrust verifies the applicant directly by the covering international organization.
- e) Evrotrust may rely on a verified professional letter to establish the applicant's information listed above, if:
 - (1) The verified professional letter includes a copy of the supporting documentation used for establishing the applicant's legal existence, such as a certificate of incorporation, memorandums of association, operating agreement, articles of association or regulatory act; and
 - (2) Evrotrust confirms the name of the applicant's organization as indicated in the Verified Professional Letter, by QIIS or QGIS.

5.4 VERIFICATION OF THE APPLICANT'S LEGAL EXISTENCE AND IDENTITY - ASSUMED (ALTERNATIVE) NAME

5.4.1 VERIFICATION REQUIREMENTS

If, in addition to the official name of the applicant as entered in the Registry or Registration Agency in the applicant's jurisdiction, the EV certificate contains all alternative names (such as "doing business as", "DBA" or "d/b/a" in the USA and "trading as" in the United Kingdom) under which the applicant conducts business, Evrotrust performs verifications of whether:

- a) the applicant has registered the use of an alternative name with the relevant government agency for such applications in the jurisdiction at its place of business, and
- b) the registration of the alternative name is still valid.

5.4.2 ELIGIBLE VERIFICATION METHOD

In order to verify each alternative name under which the applicant conducts business,

Evrotrust performs the following:

1. Evrotrust may verify the name by using a reliable national source of information managed by or on behalf of an appropriate government agency in the jurisdiction of the applicant's place of business, or through direct contact with such government agency, either personally or by post, e-mail, web address or telephone; or
2. Evrotrust may verify the alternative name by using a reliable independent source of information, provided that the QIIS has verified the presumed name with the relevant government agency.
3. Evrotrust may rely on a confirmed professional letter indicating the alternative name under which the applicant conducts business, the government agency in which the presumed name was registered, and that the registration of that name is still valid.

5.5 VERIFICATION OF THE APPLICANT'S PHYSICAL EXISTENCE

5.5.1 THE APPLICANT'S ADDRESS AND PLACE OF BUSINESS

(1) Verification requirements

In order to verify the applicant's physical existence and business presence, Evrotrust verifies whether the physical address provided by the applicant is the address at which the applicant conducts its business operations (for example, a mailbox or P.O. box or a "care of (C/O)" address is not acceptable as the address of an agent of the Organization).

(2) Eligible verification methods

A. Place of business in the country of incorporation

- (i) For applicants whose place of business is in the same country as the applicant's jurisdiction of incorporation or registration and whose place of business is not the same as that indicated in the relevant reliable national source used to verify the legal existence:
 - (1) For applicants listed at the same business address in the current version of at least one QGIS (other than that used to verify legal existence), QIIS or QTIS, Evrotrust shall confirm that the applicant's address as indicated the EV certificate application is a valid business address for the applicant by reference to such QGIS, QIIS or QTIS;
 - (2) For applicants not listed at the same business address in the current version of at least one QIIS or QTIS, Evrotrust shall confirm that the address

indicated in the EV certificate application is the applicant's address by obtaining documentation of on-site visit to the company's business address, which is to be performed by a reliable person or company. The documentation of on-site visit shall contain:

- (a) Verification of whether the applicant's company is located at the exact address indicated in the EV certificate application,
- (b) Identification of the type of the site (e.g. office in a commercial building, private residence, shop window, etc.) and whether it appears to be a permanent place of business,
- (c) It shall be indicated whether there is a permanent sign (which cannot be moved) identifying the applicant,
- (d) It shall be indicated whether there is evidence that the applicant is carrying out current business activities at the site (e.g. mailbox, etc.), and
- (e) Inclusion of one or more photographs of the exterior of the site (showing captions indicating the applicant's name, if any, and showing the street address, if possible), and the internal reception area or workspace.

- (ii) For all applicants, Evrotrust may alternatively rely on a confirmed professional letter indicating the address of the applicant's place of business.
- (iii) For government subjects, Evrotrust may rely on the address contained in the QGIS records in the applicant's jurisdiction.
- (iv) For applicants whose place of business is in the same country as the applicant's jurisdiction of incorporation or registration and where the QGIS contains a business address for the applicant, Evrotrust may rely on the QGIS address to confirm the applicant's address as specified in the EV certificate application.

B. Where the place of business is not in the country of incorporation: Evrotrust relies on a confirmed professional letter indicating the address of the applicant's place of business and that business operations are carried out there.

5.6 VERIFICATION OF THE COMMUNICATION METHOD

5.6.1 VERIFICATION REQUIREMENTS

In order to facilitate communication with the applicant and to confirm that the applicant is aware of and approves the issuance, Evrotrust verifies a telephone number, fax number, e-mail address or mailbox address as a method of communication.

5.6.2 ELIGIBLE VERIFICATION METHODS

In order to confirm the method of communication with the applicant, Evrotrust:

- A.** Verifies whether the method of communication belongs to the applicant, the company or its subsidiary, by comparing it to: the records provided by the telephone company; QGIS, QTIS or QIIS; or a verified professional letter; and
- B.** Confirms the method of communication, using it to obtain an affirmative response sufficient to reasonably conclude that the applicant, the company or its affiliate can be reliably connected by means of the verified method of communication.

5.7 VERIFICATION OF THE APPLICANT'S OPERATIONAL EXISTENCE

5.7.1 VERIFICATION REQUIREMENTS

Evrotrust verifies whether the applicant is engaged in business by verifying its operational existence. Evrotrust may rely on a verification of the legal existence of the governmental institution as an operational existence verification.

5.7.2 ELIGIBLE VERIFICATION METHODS

In order to verify the applicant's ability to engage in business, Evrotrust verifies the operational existence of the applicant or its affiliated subsidiary through:

- (1) Verification that the applicant, the affiliate, the parent or subsidiary of the applicant have existed for at least **three** years, as indicated in the Registry or Registration Agency;
- (2) Verification that the applicant, the affiliate, the parent or subsidiary of the applicant are listed in this QIIS or QTIS;
- (3) Documented verification that the applicant, the affiliate, the parent or subsidiary of the applicant have an active current deposit account with a regulated financial institution; or
- (4) Verification of a professional letter according to which the applicant has an active current

deposit account with a regulated financial institution.

5.8 VERIFICATION OF THE APPLICANT'S DOMAIN NAME

5.8.1 VERIFICATION REQUIREMENTS

- (1) For each Fully-Qualified Domain Name referred to in the certificate other than the Domain Name with .onion in the rightmost label of the domain name, Evrotrust shall confirm that at the date of issuance of the certificate, either the applicant (or its company, subsidiary or affiliate) is a Domain Name Registrant, or that it has control of the FQDN. For a certificate issued with a .onion domain name in the rightmost domain name label, Evrotrust shall confirm that at the date of issuance of the certificate, the applicant's control over the .onion domain name complies with the requirements of the Browser Forum.
- (2) **Mixed Character Set Domain Names:** EV certificates may include domain names containing mixed character sets only in accordance with the rules set by the domain registrar. Evrotrust visually compares all domain names with mixed symbol sets to known high-risk domains. If a similarity is found, the EV certificate application is marked as a high-risk one. Evrotrust carries out appropriate additional certification and verification to ensure that the applicant and the verified subject are one and the same organization.

5.9 VERIFICATION OF THE NAME, TITLE AND AUTHORITY OF THE CONTRACT SIGNATORY AND THE CERTIFICATE APPROVER

5.9.1 VERIFICATION REQUIREMENTS

For both the contract signatory and the certificate approver, Evrotrust verifies the following.

- (1) **Name, title and agency:** Evrotrust verifies the name and title of the contract signatory and the certificate approver, as the case may be. Evrotrust also verifies whether those persons are agents representing the applicant.
- (2) **Signatory authority of the contract signatory:** Evrotrust verifies that the contract signatory is authorized by the applicant to enter into a contract (and all other contractual obligations) on behalf of the applicant, including a contract specifying one or more

approval certificates on behalf of the applicant.

- (3) **EV authority of the certificate approver:** Evrotrust verifies, through a source other than the certificate approver, whether it is explicitly authorized by the applicant to do the following as of the date of the EV certificate application:

(A) To send and, where applicable, authorize the certificate applicant to apply for the EV certificate; and

(B) To provide and, where applicable, authorize a certificate applicant to provide the information from Evrotrust for the issuance of an EV certificate; and

(C) To approve the EV certificate applications submitted by the applicant.

5.9.2 ELIGIBLE VERIFICATION METHODS - NAME, TITLE AND AGENCY

The eligible methods of verifying the name, title and status of the agency of the contract signatory and certificate approver include the following.

(1) **Name and title:** Evrotrust may verify the name and title of the contract signatory and the certificate approver by any appropriate method designed to provide reasonable assurance that the person claiming to act in such a role is in fact the designated person.

(2) **Agency:** Evrotrust may verify the agency of the contract signatory and the certificate approver by:

(A) Contacting the applicant using a verified method of communication and obtaining confirmation that the contract signatory and/or the certificate approver, as applicable, is an officer of the Agency;

(B) Receiving an independent confirmation by the applicant or a verified professional letter certifying that the person is either an officer or has otherwise been appointed an agent of the applicant; or

(C) Obtainng confirmation from the QIIS or QGIS that the contract signatory and/or the certificate approver is an officer of the applicant.

Evrotrust may also verify the agency of the certificate approver through a certificate from the contract signatory (including in a contract between Evrotrust and the applicant signed by the contract signatory), provided that the employment status of the signatory in the agency has been verified.

5.9.3 ELIGIBLE VERIFICATION METHODS - COMPETENT AUTHORITY

The eligible verification methods of the signatory authority of the contract signatory and the EV authority of the certificate approver include:

- (1) **Professional letter verification:** The signatory authority of the contract signatory and/or the EV authority of the certificate approver may be verified by deciphering a verified professional letter;
- (2) **Corporate decision:** The signatory authority of the contract signatory and/or the EV authority of the certificate approver may be verified by a certified corporate decision confirming that the person has received such a signatory authority, provided that such decision has been (i) certified by the relevant corporate officer (e.g. secretary); and (ii) Evrotrust can reliably verify whether the certificate has been validly signed by that person and that he/she has the necessary power to provide such a certificate;
- (3) **Independent confirmation by the applicant:** The signatory authority of the contract signatory and/or the EV authority of the certificate approver may be verified by receiving an independent confirmation by the applicant;
- (4) **Contract between Evrotrust and an applicant:** The EV authority of the certificate approver may be verified by a contract between Evrotrust and the applicant, which designates the certificate approver with such EV authority, provided that the contract has been signed by the signatory and provided that the agency and the signatory authority have been verified;
- (5) **Previous equivalent authority:** The contract signatory's signatory power and/or the EV certificate approver's power may be verified by demonstration of a previous equivalent authority.

A. The previous equivalent authority of the signatory shall be considered confirmation or verification of the signatory power where the signatory has entered into a binding contract between Evrotrust and the applicant more than 90 days before the EV certificate application. Evrotrust shall record sufficient details of the previous agreement to correctly identify it and link it to the EV application. Such details may include any of the following:

- (i) Title of the agreement,

- (ii) Date of signing the contract,
- (iii) Reference number of the contract, and
- (iv) Place of submission.

B. A previous equivalent authority of the certificate approver may be considered confirmation or verification of the EV authority of the certificate approver where it has performed one or more of the following:

- (i) Under a contract with Evrotrust, it is an employee acting as an Enterprise RA for the applicant, or
- (ii) It has participated in the approval of one or more applications for certificates issued by Evrotrust and which are currently used and verified by the applicant. In such a case, Evrotrust will contact the certificate approver by telephone at a pre-confirmed telephone number or accept a signed and notarized letter approving the certificate application.

(6) **QIIS or QGIS:** The signatory authority of the contract signatory and/or the EV authority of the certificate approver may be verified by the QIIS or QGIS which identify the contract signatory and/or the certificate approver as a corporate officer, sole trader or other senior official of the applicant.

(7) **Representation of the contract signatory/warranty:** Provided that Evrotrust confirms that the contract signatory is an officer or agent of the applicant, Evrotrust may rely on the signatory power of the signatory by receiving a duly executed representation or warranty from the signatory, which includes the following covenants:

- A. that the applicant authorizes the signatory to sign the user agreement on its behalf,
- B. that the user agreement is valid and enforceable,
- C. that, following the performance of the user agreement, the applicant will be bound by all its terms and conditions,
- D. that the misuse of an EV certificate will have serious consequences, and
- E. that the contract signatory has the power to receive the digital equivalent of a company seal or the signature of an officer in order to establish the authenticity of the company's website.

5.9.1 RE-AUTHORIZED CERTIFICATE APPROVER

When Evrotrust and the applicant intend to submit multiple future EV certificate applications, then Evrotrust shall:

- (1) verify the name and title of the contract signatory and the fact that it is an officer or agent of the applicant; and
- (2) verify the signatory authority of such contract signatory in accordance with any of the above procedures. Evrotrust and the applicant may enter into a written agreement signed by the contract signatory on behalf of the applicant, in which case, for a certain period of time, the applicant expressly authorizes one or more certificate approvers to exercise EV powers in respect of any future certificate request submitted on behalf of the applicant and duly certified. Such an agreement shall provide that the applicant will be required under the user agreement for all EV certificates to include provisions for: (i) verification of the certificate approver, (ii) periodic re-validation of the EV authority of the certificate approver, (iii) secure procedures under which the applicant may notify Evrotrust that the EV authority of any certificate approver has been revoked; and (iv) any other appropriate safeguards which may be reasonably necessary.

5.10 VERIFICATION OF SIGNATURE ON A USER CONTRACT AND EV CERTIFICATE APPLICATIONS

Both the user agreement and any unauthorized EV certificate application shall be signed. The agreement shall be signed by an authorized signatory. The EV certificate application shall be signed by the certificate applicant submitting the document, unless the certificate application has been previously authorized. If the certificate applicant is not authorized to approve the certificate, then the application shall be approved by an independent authorized certificate approver. In any case, the applicable signatures shall be legally valid, thus binding the applicant to the terms and conditions of each relevant document.

5.10.1 VERIFICATION REQUIREMENTS

- (1) **Signature:** Euvotrust shall certify the signature of the contract signatory and the signature of the certificate applicant on every EV certificate application in a manner that guarantees that the person indicated as the signatory in the applicable document is in fact the person who signed the document on behalf of the applicant.

- (2) **Alternative approval:** In cases where an EV certificate application has been signed and submitted by the certificate applicant who does not act as the certificate approver as well, then an approval and acceptance of the EV certificate application by a certificate approver may replace the certification of the applicant's signature on such an EV certificate application.

5.10.2 ELIGIBLE SIGNATURE VERIFICATION METHODS

The eligible methods for certifying the signature of the applicant or the contract signatory include the following:

- (1) Contacting the applicant by using a verified method of communication followed by a response from someone who identifies itself as such person, confirming that he/she has signed an applicable document on behalf of the applicant;
- (2) A letter sent to the address of the applicant or agent, confirmed by independent means in accordance with this document with a subsequent response from someone who identifies itself as such person, confirming that he/she has signed the applicable document on behalf of the applicant;
- (3) Use of a signature process that establishes the name and title of the signatory in a secure manner, for example, by using an appropriate secure entry process that identifies the signatory prior to signing, or by using a digital signature made with reference to an appropriately verified certificate; or
- (4) Notarization, provided that Evrotrust independently verifies whether such a notary is legally qualified in the jurisdiction of the applicant or the contract signatory.

5.11 VERIFICATION OF APPROVAL OF AN EV CERTIFICATE APPLICATION

5.11.1 VERIFICATION REQUIREMENTS

In cases where an EV certificate application has been submitted by a certificate applicant before Evrotrust issues the requested EV certificate, Evrotrust shall verify whether the authorized certificate approver has reviewed and approved the EV certificate application.

5.11.2 ELIGIBLE VERIFICATION METHODS

The eligible methods for verifying the approval of an EV certificate application include:

- (1) Contacting the certificate approver through a verified method of communication with the applicant and receiving oral or written confirmation that the certificate approver has reviewed and approved the EV certificate application;
- (2) Notification of the certificate approver that one or more new EV certificate applications are available for review and approval on a given website with controlled access and protection, followed by the certificate approver's entry and giving approval as required by the website; or
- (3) Verification of the certificate approver's signature on the EV certificate application in accordance with this document.

5.12 VERIFICATION OF CERTAIN SOURCES OF INFORMATION

5.12.1 VERIFICATION OF LEGAL OPINION

- (1) **Verification requirements:** Before referring to a legal opinion, Evrotrust verifies whether it meets the following requirements:
 - A. **Author status:** Evrotrust verifies whether the legal opinion was compiled by an independent lawyer hired by and representing the applicant (or an in-house lawyer) who is either:
 - (i) an attorney-at-law licensed to practice law in the country in which the applicant's jurisdiction is, or in any jurisdiction in which the applicant maintains an office or a physical site, or
 - (ii) a Latin Notary who is currently authorized or licensed to practice in the country of the applicant's jurisdiction of incorporation or registration or in any jurisdiction in which the applicant maintains an office or a physical site (and that such jurisdiction recognizes the role of a Latin Notary);
 - B. **Grounds for the opinion:** Evrotrust verifies that the lawyer is acting on behalf of the applicant and that the conclusions contained in the verified legal opinion are based on the

lawyer's declared knowledge of the relevant facts, professional judgment and expertise;

C. **Authenticity:** Evrotrust confirms the authenticity of the verified legal opinion.

(2) **Eligible verification methods:** The eligible methods for establishing the above requirements for a verified legal opinion are:

A. **Author status:** Evrotrust verifies the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing the lawyer in the applicable jurisdiction;

B. **Grounds for the opinion:** The text of the legal opinion shall clearly state that the lawyer is acting on behalf of the applicant and that the conclusions of the legal opinion are based on knowledge of the relevant facts, exercise of professional judgment and experience on the part of the practitioner. The legal opinion may also include a disclaimer and other limitations common in the lawyer's jurisdiction, provided that the scope of the declared disclaimer is not so large as to eliminate any significant risk (financial, professional and/or reputational) for the lawyer, if the legal opinion turns out to be wrong;

C. **Authenticity:** In order to confirm the authenticity of the legal opinion, Evrotrust makes a telephone call or sends a copy of the legal opinion back to the address, telephone number, fax or e-mail of the Legal Practitioner responsible for registering or licensing the legal practitioner, and receiving confirmation that the legal opinion is authentic. If no telephone number is made available by the licensing authority, Evrotrust may use any numbers indicated for contact with the Legal Practitioner in records provided by the applicable telephone company, QGIS or QIIS.

In case the opinion was signed digitally, in a way that confirms the authenticity of the document and the identity of the signatory, no additional authentication is required.

5.12.2 VERIFICATION OF ACCOUNTING LETTER

(1) **Verification requirements:** Before referring to an accounting letter, Evrotrust shall verify whether such accounting letter meets the following requirements:

- A. **Author status:** Evrotrust shall confirm that the author of the accounting letter is a financier who works for the applicant and is licensed in the country where applicant's jurisdiction of incorporation or registration is, or a country where the applicant maintains an office or physical site. The verification of the license is carried out by the member organization or the regulatory organization in the accountant's country or jurisdiction. Such a country or jurisdiction shall have an accounting standards authority that maintains a full membership status in the International Federation of Accountants.
- B. **Grounds for the opinion:** Evrotrust verifies whether the accountant is acting on behalf of the applicant and that the conclusions contained in the letter are based on the accountant's declared knowledge of the relevant facts, professional judgment and expertise;
- C. **Authenticity:** Evrotrust shall confirm the authenticity of the accountant's letter.
- (2) **Eligible verification methods:** The acceptable methods for establishing the above requirements for the accountant's letter include:
- A. **Author status:** Evrotrust shall verify the professional status of the author of the accounting letter by directly contacting the authority responsible for registering or licensing such accountants in the applicable jurisdiction.
- B. **Grounds for the opinion:** The text of the verified accountant's letter shall clearly state that the accountant is acting on behalf of the applicant and that the information in the letter is based on the accountant's stated knowledge of the relevant facts, professional judgment and expertise. The verification may also include a disclaimer and other limitations common to the accountant's jurisdiction, provided that the scope of the declared disclaimer is not so large as to eliminate any material risk (financial, professional and/or reputational) for the accountant if the verified accountant's letter turns out to be wrong.
- C. **Authenticity:** In order to confirm the authenticity of the accountant's opinion, Evrotrust

shall make a telephone call or send a copy of the verified accountant's letter back to the accountant's address as indicated by the authority responsible for registering or licensing such accountants, receiving confirmation by the accountant or assistant accountant that the accountant's letter is authentic. If no telephone number is made available by the licensing authority, Evrotrust may use the number indicated for contact with the accountant in the records provided by the applicable telephone company, QGIS or QIIS.

In case the opinion was signed digitally, in a way that confirms the authenticity of the document and the identity of the signatory, no additional authentication is required.

5.12.3 FACE-TO-FACE VERIFICATION

- (1) **Verification requirements:** Before relying on Face-to-Face when verifying the documents submitted, Evrotrust shall verify whether the Third-Party Validator meets the following requirements:
 - A. **Qualification of the third party validator:** Evrotrust shall perform an individual verification of whether the third party validator is a legally qualified Latin Notary or other type of notary (or legal equivalent in the applicant's jurisdiction), attorney-at-law or accountant in the jurisdiction of the person's residence;
 - B. **Document Custody Chain:** Evrotrust confirms that the validator has reviewed the documents during a face-to-face with a certified person;
 - C. **Attestation Verification:** If the third party validator is not a Latin Notary, then Evrotrust confirms the authenticity of the attestation documents.
- (2) **Eligible verification methods:** The eligible methods for establishing the above requirements for verification of documents are:
 - A. **Qualification of the third party validator:** Evrotrust verifies the professional status of the third party validator by directly contacting the authority responsible for registering or licensing such validators in the applicable jurisdiction;

- B. **Document Custody Chain:** The third party validator shall submit a declaration to Evrotrust certifying that it has received the documents to be verified during a face-to-face meeting with the person;
- C. **Attestation Verification:** If the third party validator is not a Latin Notary, then the Evrotrust shall confirm the authenticity of the documents received for verification. Evrotrust shall make a telephone call to the third party validator and receive confirmation from it or its assistant that face-to-face validation has been carried out. In cases where the attestation was signed digitally, in a way that confirms the authenticity of the documents and the identity of the signatory, no additional authentication is required.

5.12.4 INDEPENDENT CONFIRMATION BY THE APPLICANT

Independent confirmation by the applicant is a confirmation of a specific fact (e.g. confirmation of the status of an officer or agency in the contract or the certificate approver, confirmation by the EV authority approving the certificate, etc.), which:

- A. Was received by Evrotrust (from someone other than the person being verified) who has the appropriate power to confirm such a fact and who provides evidence of the confirmation;
- B. Was received by Evrotrust in a way that certifies and verifies the source of the confirmation; and
- C. Is binding to the applicant.

Independent confirmation by the applicant may be obtained through the following procedure:

- (1) **Confirmation request:** Evrotrust shall initiate a confirmation request through appropriate communication beyond the scope, requesting verification or confirmation of the specific disputed fact, as follows:

- A. **Addressee:** The confirmation request shall be addressed to:

- (i) A position within the applicant's organization that qualifies as a validator (e.g.

Secretary, President, Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Chief Executive Officer, CSO, Director, etc.) and is identified by name and position in a current QGIS, QIIS, QTIS, Verified Legal Opinion, Verified Accounting Letter or by contacting the applicant via a Verified Communication Method; or

(ii) The registered agent or registered office of the applicant in the jurisdiction of incorporation, as listed in the official registers of the Registry Agency, with instructions for it to be sent to an appropriate validator; or

(iii) A designated person who has been confirmed to be in direct line of management above the contract signatory or the certificate approver, by contacting the applicant's Human Resources Department by telephone or post.

B. Communication methods: The confirmation request shall be addressed to the validator in a way that is reasonably likely to reach that person. The following options are allowed:

(i) By paper mail, to:

- (1) The address of the applicant's place of work as confirmed by Evrotrust in accordance with this document, or
- (2) The validator's business address as specified in a current QGIS, QTIS, QIIS, Verified Professional Letter, or
- (3) The address of the applicant's registered agent or registered office as indicated in the official registers of the jurisdiction of incorporation, or

(ii) by e-mail, addressed to the validator at the official e-mail address of that person as indicated in a current QGIS, QTIS, QIIS, verified legal opinion or confirmed accounting letter; or

(iii) by telephone call to the validator at the principal telephone number of the applicant's place of business (confirmed in accordance with this document) requesting that the said person be identified; or

(iv) by fax to the validator at the place of business. The fax number shall be specified in a current QGIS, QTIS, QIIS, verified legal opinion or verified accounting letter. The

title page shall be clearly addressed to the validator.

(2) Confirmatory response: Evrotrust shall receive a response to the request from the person confirming the specific disputed fact. Such a response may be delivered to Evrotrust by telephone, e-mail or on paper, as long as Evrotrust can reliably verify that it has been sent by the validator in response to the request.

(3) Evrotrust may rely on a person for confirmation, to confirm its own contact information: e-mail address, telephone number and fax number. Evrotrust may rely on verified contact information for future correspondence with the validator if:

- A. The domain of the e-mail address is the property of the applicant and is the validator's own e-mail address, and not a group e-mail pseudonym;
- B. The telephone/fax number of the validator is verified by Evrotrust that it is a telephone number which is part of the organization's telephone system and is not the person's personal telephone number.

5.12.5 RELIABLE INDEPENDENT INFORMATION SOURCE

The Qualified Independent Information Source (QIIS) is a regularly updated and publicly available database that is generally recognized as a reliable source of certain information. The database qualifies as a QIIS if Evrotrust determines that:

- (1) Industries other than the sector of certification service providers rely on the database for exact location, contact or other information; and
- (2) The database provider updates its data at least once a year.

Evrotrust uses a documented process to verify the accuracy of the database and to ensure that its data is acceptable, including a review of the database provider's conditions of use. Evrotrust does not use data in a QIIS that it knows to:

- (i) be self-reported, and
- (ii) have not been verified by the QIIS as accurate.

5.12.6 RELIABLE GOVERNMENTAL INFORMATION SOURCE

The Qualified Governmental Information Source (QGIS) is a regularly updated, publicly available database created for the purpose of accurately providing information and which is

recognized as a reliable source of such information, provided that it is lawfully maintained by a governmental institution. This document does not prohibit the use of third parties to obtain information, provided that such third party receives the information directly from the governmental institution.

5.12.7 RELIABLE SOURCE OF GOVERNMENT TAX INFORMATION

A qualified source of government tax information is a reliable source of government information that specifically contains tax information related to private organizations, business entities, or natural persons.

5.13 OTHER VERIFICATION REQUIREMENTS

5.13.1 REFUSAL LISTS AND OTHER LEGAL BLOCKING LISTS

(1) **Verification requirements:** Evrotrust verifies whether the applicant, the contract signatory, the certificate approver, the applicant's jurisdiction of incorporation, registration or place of business:

- A. are identified in the government's refusal list, the list of banned persons or any other list that prohibits the conduct of business with such an organization or person under the national laws; or
- B. have their jurisdiction of incorporation, registration or place a business in any country with which the Bulgarian law prohibits the conduct of business.

Evrotrust will not issue EV certificates to an applicant if the applicant, the contract signatory, the certificate approver, the applicant's jurisdiction of incorporation or registration or place of business is on such a list.

(2) **Eligible verification methods:** Evrotrust shall take reasonable verification steps in any other country with all equivalent refusal lists.

5.13.2 PARENT / SUBSIDIARY / AFFILIATE RELATIONS

Evrotrust verifies the applicant using information about the applicant's parent or subsidiary or affiliate, and verifies the applicant's relationship with that company. The eligible verification methods include:

- (1) QIIS or QGIS: The relationship between the applicant and the company is identified

- in a QIIS or QGIS;
- (2) Independent confirmation by the company: Evrotrust may verify the relationship between the applicant and the company by obtaining an independent confirmation;
 - (3) Contract between Evrotrust and the company, or the affiliate: Evrotrust verifies the relationship between the applicant and the company through a contract between the former and the company which determines the certificate approver with such EV authority, provided that the contract has been signed by the contract signatory and provided that the agency and the authority of the contract signatory have been verified;
 - (4) Verification of a professional letter: Evrotrust may verify the relationship between the applicant and the company or affiliate through a verification of a professional letter; or
 - (5) Corporate decision: Evrotrust may verify the relationship between an applicant and a subsidiary by relying on a certified corporate decision approving the establishment of the subsidiary or the applicant, provided that such decision
 - (i) has been certified by the relevant corporate officer (e.g. secretary); and
 - (ii) Evrotrust may reliably verify that the certificate has been validly signed by such person and that the said person has the necessary power to provide such certification.

5.14 FINAL CROSS-CORRELATION AND DUE DILIGENCE

Save for Enterprise EV certificates:

- (1) The results of the verification procedures described in this document are intended to be reviewed both individually and in aggregate. Thus, once all verification procedures have been completed, Evrotrust must have a person who is not responsible for collecting information, but reviews all information and documentation collected in support of the EV certificate application and looks for any discrepancies or missing data.
- (2) Evrotrust will receive and document additional explanations or

clarifications from the applicant, the certificate approver, the applicant, the reliable independent information source and/or any other sources of information, if necessary to resolve such discrepancies or request any additional information.

(3) Evrotrust refrains from issuing EV certificates until all information and documentation collected in support of the EV certificate application has been confirmed. If satisfactory explanations and/or additional documentation are not received within a reasonable time, Evrotrust will reject the application and notify the applicant accordingly.

(4) In the event that part or all of the documentation used in support of the application is in a language other than the normal operating language of Evrotrust and the officers do not have the language skills sufficient to perform the final cross-correlation and due diligence, Evrotrust will rely on language translations of the relevant parts of the documentation, provided that such translations are obtained by a sworn translator.

5.15 REQUIREMENTS FOR THE RE-USE OF EXISTING DOCUMENTATION

For each EV certificate application, including requests for renewal of existing EV certificates, Evrotrust performs all certification and verification procedures as required by this document in order to ensure that the application has been duly authorized by the applicant and that the information contained in the EV certificate is still accurate and valid.

5.15.1 VERIFICATION FOR EXISTING SUBSCRIBERS

If the applicant has a valid EV certificate issued by Evrotrust, Evrotrust relies on its prior certification and verification of:

- (1) The main person verified according to this document as a natural person is the same person who has already been certified;
- (2) The applicant's place of business according to this document;
- (3) Verified method of communication of the applicant, which is to be confirmed;
- (4) The applicant's operational existence;

(5) The name, title, agency and authority of the contract signatory and certificate approver; and

(6) The applicant's right to use the domain name indicated under this document, provided that Evrotrust has certified that the WHOIS record still shows the same registrant as at the time Evrotrust certified the indicated domain name for the original EV certificate.

5.15.2 REQUESTS FOR RE-ISSUE

Evrotrust relies on a pre-verified certificate application to issue a replacement certificate, as long as the referenced certificate has not been terminated due to fraud or any other illegal conduct if:

(1) The period of validity of the reissued certificate shall be the same as the expiry date of the EV certificate to be replaced, and

(2) The information about the subject of the certificate is the same as the subject in the EV certificate to be replaced.

5.15.3 VALIDITY PERIOD OF THE VERIFIED DATA

(1) Save for reissued EV certificates and where otherwise decided, the validity of all data used in support of the issuance of EV certificates shall not exceed the following limits:

(A) Legal existence and identity - thirteen months;

(B) Presumed name - thirteen months;

(C) Business address - thirteen months;

(D) Proven method of communication - thirteen months;

(E) Operational existence - thirteen months;

(F) Domain name - thirteen months;

(G) Name, title, agency and authority - thirteen months, unless a different period is stipulated in the contract between Evrotrust and the applicant, in which case the period stipulated in such contract shall be controlled.

(2) The thirteen-month period referred to above shall start to run from the date on which the information was collected by Evrotrust.

(3) Evrotrust may use a re-submitted EV certificate application, user contract or General

Terms and Conditions, including the use of a single EV certificate application in support of multiple EV certificates containing the same subject, to the extent permitted by this document.

(4) Evrotrust shall repeat the verification process required in this document for every information received beyond the periods referred to above, unless otherwise agreed.

6 OPERATIONAL REQUIREMENTS

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

6.1 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".

6.1.1 WHO CAN APPLY FOR A QUALIFIED CERTIFICATE

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

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

6.1.2.1 USER CERTIFICATES

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

6.1.2.2 CERTIFICATES OF CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY

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

6.1.2.3 REQUEST FOR REGISTRATION OF USERS OF QUALIFIED TRUST SERVICES

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

6.1.2.4 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".

Evrotrust may renew a valid qualified certificate which has not been terminated within its validity period, by generating a new key pair (Re-key). Evrotrust does not support renewal by preserving the existing key pair or by preserving the serial number.

Evrotrust renews a current certificate of the Holder/Creator with a new key pair (Re-key), only if there are no changes in the certified information. The renewed certificate has a new serial number entered therein, a new public key, a new period of validity and a new electronic signature/seal by the certification authority, the information certified in it being preserved.

Following renewal, the current qualified certificate shall not be terminated and shall remain valid for the period of its validity.

Existing evidence may be used to re-verify identity depending on the applicable law and in consideration of the fact that the evidence collected has remained valid given the time that has elapsed.

For identification and verification of the identity of the Holder/Creator of the qualified certificate being renewed, its personal appearance before the Evrotrust registration authority is not required.

In case of any changes in the information about the Holder/Creator of a qualified certificate, the current certificate shall not be renewed. The provider shall issue a new qualified certificate, following an initial identification and verification of identity, and shall immediately terminate the current qualified certificate.

6.1.2.5 REQUEST FOR SUSPENSION AND TERMINATION OF A CERTIFICATE

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

Evrotrust provides an opportunity for users to request the termination of their own certificates. The process is described in this document. Evrotrust supports a 24x7 process for accepting and responding to termination requests and reporting certificate-related problems.

Evrotrust provides users, relying parties, application software providers and other third parties with clear instructions on how to report suspected private key compromise, certificate misuse or other types of certificate-related fraud. The instructions are public and easily accessible through online means.

6.2 PROCESSING OF THE REQUEST

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

6.2.1 PERFORMING IDENTIFICATION AND ESTABLISHING IDENTITY

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

6.2.2 ACCEPTANCE OR REJECTION OF A REQUEST

6.2.2.1 PROCESSING OF A REQUEST BY THE REGISTRATION AUTHORITY

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

6.2.2.2 PLACING A REQUEST WITH THE CERTIFICATION AUTHORITY FOR THE ISSUANCE OF A QUALIFIED CERTIFICATE

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

6.2.3 AWAITING FOR THE ISSUANCE OF A QUALIFIED CERTIFICATE

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

6.2.4 THE CERTIFICATION AUTHORITY AUTHORIZES DATA PROCESSING

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

6.3 ISSUANCE OF A QUALIFIED CERTIFICATE

6.3.1 PROCESSING

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

The issuance of a certificate by a Root CA is performed by an authorized officer of Evrotrust (system operator or PKI administrator).

6.3.2 PROVIDING INFORMATION

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

6.4 ACCEPTANCE OF A QUALIFIED CERTIFICATE

6.4.1 CONFIRMATION FOR ACCEPTANCE OF A QUALIFIED CERTIFICATE

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

6.4.2 PUBLICATION OF A QUALIFIED CERTIFICATE

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

6.4.3 INFORMATION INTENDED FOR OTHER PARTIES

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

6.5 USE OF A QUALIFIED CERTIFICATE AND A KEY PAIR

6.5.1 BY USERS

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

The maximum validity period for an EV certificate shall not exceed **398 days**. In its activities of issuing EV certificates, Evrotrust applies the the recommendations of the EV Guidelines for a

maximum period of validity **of twelve (12) months**.

6.5.2 BY RELYING PARTIES

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

6.6 RENEWAL OF A QUALIFIED CERTIFICATE

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

6.7 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".

6.7.1 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".

6.7.2 PERSONS AUTHORIZED TO REQUEST AN UPDATE OF A KEY PAIR

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

6.7.3 RE-KEY AND PROCESSING OF THE REQUEST

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

Evrotrust accepts requests for re-issuance of EV certificates in cases where the certificates referred to have not been revoked due to fraud or other illegal conduct. Evrotrust may rely on a pre-verified application for a new certificate if:

- a)** the period of validity of the reissued certificate is the same as the expiry date of the EV certificate being replaced, and

- b) the information about the subject of the certificate is the same as in the old EV certificate.

Evrotrust complies with the requirements for requests for re-issuance of certificates. The period of validity of the verified data shall not exceed 13 (thirteen) months, unless otherwise agreed, and as described in item 5.15.3 of this document.

6.7.4 USER INFORMATION

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

6.7.5 CONFIRMATION OF ACCEPTANCE OF A NEW CERTIFICATE

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

6.7.6 PUBLICATION OF A NEW QUALIFIED CERTIFICATE

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

6.7.7 INFORMATION INTENDED FOR THE RELYING PARTIES

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

6.8 CHANGE IN A QUALIFIED CERTIFICATE

6.8.1 REASONS FOR THE CHANGE IN A QUALIFIED CERTIFICATE

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

Requests for changes in certificates issued to subjects that have previously been registered shall be complete and accurate. The procedure involves updating the certificate due to a change in the user's attributes.

If any certified names or attributes have changed, or the previous certificate has been terminated, the registration information will be verified, recorded, and agreed with the user.

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

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

6.8.3 PROCESSING OF THE REQUEST

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

6.8.4 USER INFORMATION

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

6.8.5 CONFIRMATION OF ACCEPTANCE OF A NEW QUALIFIED CERTIFICATE

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

6.8.6 PUBLICATION OF A NEW QUALIFIED CERTIFICATE

Evrotrust, through the operational certification authority, publishes the changed qualified certificate immediately in the the register of certifications.

6.8.7 INFORMATION INTENDED FOR THE RELYING PARTIES

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

6.9 SUSPENSION AND TERMINATION OF A QUALIFIED CERTIFICATE

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

Evrotrust shall terminate certificates in a timely manner on the basis of authorized and validated applications. Evrotrust shall terminate any valid certificate:

- a) which is no longer in accordance with the policy under which it was issued;

- b) Evrotrust is aware of any changes that have affected the validity of the certificate; or
- c) for which the cryptography used no longer provides a reliable connection between the holder and the public key.

The subject and, where applicable, the user of a terminated or suspended certificate shall, where possible, be informed of any change in the status of the certificate.

Once the certificate has been permanently terminated (i.e. not suspended), it cannot be reinstated.

6.9.1 CIRCUMSTANCES FOR TERMINATION OF A QUALIFIED CERTIFICATE

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

Evrotrust provides an opportunity for users to request the suspension of their own certificates 24x7.

Evrotrust shall suspend a user's certificate within 24 hours if one or more of the following reasons exist:

- a) The user requests in writing that Evrotrust suspends the certificate;
- b) The user notifies Evrotrust that the original certificate application was not authorized and does not grant a retroactive authorization;
- c) Evrotrust receives evidence that the user's private key corresponding to the public key in the certificate has been compromised;
- d) Evrotrust has identified the user's private key as a weak key;
- e) Evrotrust has received evidence that authorization validation or domain control for each Fully-Qualified Domain Name or IP address in the certificate should not be relied upon.

6.9.2 WHO MAY REQUIRE TERMINATION OF A QUALIFIED CERTIFICATE?

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

The user, RA or Evrotrust may initiate the termination of a certificate. Moreover, users, relying parties, application software providers, and any other third parties may submit reports on

certificate-related problems and reasonable reasons for the suspension thereof.

6.9.3 PROCEDURE FOR TERMINATION OF A QUALIFIED CERTIFICATE

6.9.3.1 PROCEDURE FOR TERMINATION OF A QUALIFIED END USER CERTIFICATE

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

Evrotrust shall suspend the validity of a certificate within 24 hours and terminate a certificate within 7 days if one or more of the following circumstances have been established:

- a. The certificate no longer meets the BRG requirements;
- b. Evrotrust has received evidence of misuse of the certificate;
- c. Evrotrust has been notified that a user had breached one or more of its obligations under its Contract with Evrotrust or the General Terms of Use;
- d. Evrotrust has been informed of any circumstance indicating that the use of a Fully-Qualified Domain Name or IP address in the certificate is no longer permitted by law;
- e. Evrotrust has been informed that the Wildcard Certificate had been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- f. Evrotrust has been notified of any significant change in the information contained in the certificate;
- g. Evrotrust has been notified that the certificate had not been issued in accordance with the BRG requirements or Evrotrust Policy and Practice;
- h. Evrotrust establishes or has been informed that the information appearing in the certificate is incorrect;
- i. Evrotrust's right to issue certificates expires, is suspended or terminated, unless Evrotrust has taken measures to continue to maintain the CRL/OCSP repository;
- j. Termination is required in accordance with Evrotrust Policy and Practice; or
- k. Evrotrust has information that the user's private key has been compromised or there is clear evidence that the method used to generate the private key was wrong.

6.9.3.2 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".

Evrotrust shall suspend the validity of a Subordinate CA certificate within seven (7) days if one or more of the following circumstances occur:

- a. The Certification Authority requires termination in writing;
- b. The Certification Authority notifies Evrotrust that the original certificate application has not been authorized and it does not grant its authorization retroactively;
- c. Evrotrust obtains evidence that the private key of the Certification Authority corresponding to the public key in the certificate has been compromised or no longer meets the regulatory requirements;
- d. Evrotrust receives evidence of misuse of the certificate;
- e. Evrotrust has been informed that the certificate had not been issued in accordance with this document or that the Certification Authority had not complied with the requirements of this document or the applicable Policy and Practice;
- f. Evrotrust establishes that the information appearing in the certificate is inaccurate or misleading;
- g. Evrotrust or the Subordinate CA wind up their activities for any reason and have not agreed another certification authority to perform the certificate management;
- h. The right of Evrotrust or the Subordinate CA to issue certificates expires, is revoked or terminated, unless Evrotrust has taken measures to continue to maintain the CRL/OCSP repository; or
- i. Termination is required by the Evrotrust Policy and Practice for the issuance of certificates.

6.9.4 GRACE PERIOD OF TERMINATION OF A QUALIFIED CERTIFICATE

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

The maximum delay between the receipt of a request for suspension or termination of a

certificate and the decision to change its status information allowed to all relying parties shall be a maximum of 24 hours. If the request for termination or suspension cannot be confirmed within 24 hours, then the status will not be changed.

The maximum delay between the confirmation of the suspension or termination of a certificate in order to take effect and the actual change of the status information of such certificate allowed to relying parties shall be a maximum of 60 minutes.

6.9.5 TIME LIMITS FOR PROCESSING OF THE TERMINATION REQUEST

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

Within 24 hours of receiving a report on a certificate-related problem, Evrotrust shall investigate the facts and circumstances related to the report and provide a preliminary report containing its findings to both the user and the person who submitted the report on a certificate-related problem. The period from the receipt of the report on a certificate-related problem or a termination-related notice to the published termination shall not exceed the period referred to in this document. The date chosen by Evrotrust shall be complied with:

- a) The nature of the alleged problem (scope, context, severity, magnitude, risk of damage);
- b) The consequences of termination (direct and additional effects on users and relying parties);
- c) The number of reports on certificate-related problems for a particular certificate or user;
- d) The subject who submitted the complaint; and
- e) The relevant applicable law.

If a termination request is related to a planned termination, regulated procedures with a predetermined period of validity shall be performed.

At its own discretion, Evrotrust may set a short period of time for the termination process.

The time used to provide termination services shall be synchronized with UTC at least once every 24 hours.

Evrotrust processes termination requests and reports on termination events. Termination requests and reports on termination events shall be established and verified for whether they

have been submitted by an authorized source.

6.9.6 CHECK OF THE CERTIFICATE REVOCATION LIST (CRL)

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

The repository does not include records indicating that a certificate has been suspended.

6.9.7 FREQUENCY OF ISSUING THE CERTIFICATE REVOCATION LIST (CRL)

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

6.9.8 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).

6.9.9 ONLINE VERIFICATION OF THE CERTIFICATE STATUS

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

Evrotrust uses Certificate Revocation Lists (CRLs) which are published at least every 24 hours. A CRL specifies the time for the next scheduled issuance. A new CRL may be published before the specified time. The CRL shall be signed by the Evrotrust Certification Authority.

Evrotrust maintains up-to-date information on the status of its certificates.

Evrotrust maintains the availability of CRL and OCSP services, which provide a response time of ten seconds or less under normal operating conditions. Evrotrust keeps an online 24x7 repository which can be used by the application software to automatically verify the current status of all unexpired certificates. Evrotrust maintains ongoing support (24x7) for the services in order to respond adequately and quickly to a certificate-related problem and, where appropriate, to forward any complaints received to the legislative bodies and/or terminate a certificate that is the subject of such a complaint.

Evrotrust ensures that upon termination of EV certificates, the CRL can be downloaded in

no more than three (3) seconds over an analog telephone line under normal network conditions.

6.9.10 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>.

Termination status information is available 24 hours a day, 7 days a week. In the event of failure of the system, the service or any other factors beyond the control of Evrotrust, Evrotrust will make every effort to ensure that this information service will not be available for longer than the maximum period of time specified in the General Terms and Conditions or the user contract. Evrotrust applies procedures to protect the integrity and authenticity of status information. The termination status information includes information on a certificate status at least until the expiry of the period of validity of such certificate.

The termination status information methods supported by Evrotrust are OCSP or CRL and are available without any geographical boundaries.

6.9.11 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.

6.9.12 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.

6.9.13 PERSONS AUTHORIZED TO REQUEST THE SUSPENSION OF A QUALIFIED CERTIFICATE

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

6.9.14 PROCEDURE FOR SUSPENSION AND RESUMPTION OF A QUALIFIED CERTIFICATE

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

6.9.15 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.

6.9.16 RESUMPTION OF A SUSPENDED CERTIFICATE

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

6.9.17 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.

6.10 CHECKING THE CURRENT STATUS (STATUS) OF QUALIFIED CERTIFICATES

6.10.1 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).

6.10.2 ADDITIONAL FUNCTIONS

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

6.11 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".

6.12 PRIVATE KEY ESCROW

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

7 CONTROL OVER THE PHYSICAL AND ORGANIZATIONAL SECURITY

Evrotrust's security requirements for network connectivity and the certification system fully meet the requirements of the Browser Forum.

Evrotrust has developed, implemented and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity and availability of certificate data and certificate management processes;
2. Protect the confidentiality, integrity and accessibility of certificate data and certificate management processes against expected threats or dangers;
3. Protect against unauthorized or illegal access, use, disclosure, alteration or destruction of any certificate data or certificate management processes;
4. Protect against accidental loss, destruction or damage of any certificate data or certificate management processes; and
5. Comply with all other lawful security requirements.

The certificate management process includes:

1. physical security and environmental control;
2. control of the system's integrity, including configuration management, maintenance of the integrity of a reliable code and detection/prevention of malicious software;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, which includes individual tasks with a trusted role, education, awareness and training; and

5. logical access control, registration of activities and lack of activity in order to ensure individual accountability.

Evrotrust Information Security Plan includes an annual risk assessment that:

1. Identifies foreseeable internal and external threats that may lead to unauthorized access, disclosure, misuse, alteration or destruction of any certificate data or certificate management processes;
2. Assesses the likelihood of and potential damage from such threats, taking into account the sensitivity of certificate data or certificate management processes; and
3. Assesses the adequacy of the policies, procedures, information systems, technologies and other arrangements that Evrotrust has in place to counter such threats.

Based on the risk assessment, Evrotrust develops, implements and maintains an information security plan consisting of security procedures, measures and products designed to achieve the objectives set out above and to manage and control the risks identified during the risk assessment commensurate with the sensitivity of the certificate data or certificate management processes. The information security plan includes administrative, organizational, technical and physical safeguards appropriate to the sensitivity of the certificate data or certificate management processes. The plan takes into account the technology available, the cost of implementing specific measures and their reasonable application according to the level of security appropriate to the damage that may result from any breach of security and the nature of the data to be protected.

7.1 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, ISO 19001:2013.

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

7.1.1 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.

7.1.2 PHYSICAL ACCESS

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

7.1.3 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.

7.1.4 WASTE DISPOSAL

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

7.2 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.

7.2.1 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.

Only employees with trusted roles may archive, store and restore the private keys of Evrotrust Certification Authorities and certification services.

All personnel with trusted roles shall maintain skill levels in accordance with the completed

educational degree and training programs.

7.2.2 REQUIREMENTS FOR THE SEPARATION OF DUTIES

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

7.3 PERSONNEL CONTROL

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

Before engaging any person in the certificate management process, whether as an employee, agent or independent contractor of Evrotrust, Evrotrust verifies the identity and reliability of that person.

Evrotrust checks the personnel of a delegated third party involved in the issuance of certificates as to whether they have completed training and whether they have the skills to store documents and record events.

7.3.1 REQUIREMENTS FOR THE TRAINING OF EVROTRUST PERSONNEL

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

Evrotrust provides all information verification personnel with training covering basic knowledge of the public key infrastructure, authentication and verification policies and procedures (including Policy and Practice), general threats to the information verification process (including phishing and other techniques).

Evrotrust keeps records of the trainings conducted to ensure that the personnel charged with the duties of validation specialists maintain a level of skills that allows them to perform such duties to a satisfactory level. Evrotrust requires a training protocol before allowing validation personnel to perform their duties.

Evrotrust requires that all officers of the Registration Authority performing validation functions pass an internal examination into the information verification requirements as set out in this document.

7.4 RECORDING EVENTS AND MAINTAINING JOURNALS

Archived journals are kept for at 10 (ten) years.

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

7.4.1 EVENT RECORDS

Evrotrust and each delegated third party shall record details of the actions taken to process certificate applications and to issue certificates, including all information generated and documentation received in connection with the application; the time and date; and the personnel involved. Evrotrust makes these records available to auditors who verify compliance with the requirements of this document.

Evrotrust records at least the following events:

1. Evrotrust certificates and key events related to the life cycle of those certificates, including:
 - a) Key generation, backup, storage, recovery and destruction;
 - b) Certificate applications, requests for renewal and rekey and termination;
 - c) Approval and rejection of certificate applications;
 - d) Cryptographic device lifecycle management events;
 - e) Generation of CRL and OCSP records;
 - f) Introduction of new certificate profiles and withdrawal of existing certificate profiles.
2. Events related to user certificate lifecycle management, including:
 - a) Certificate applications, requests for renewal and rekey and termination;
 - b) All verification activities provided for in this document and the Evrotrust Practice;
 - c) Approval and rejection of certificate applications;
 - d) Issuance of certificates; and
 - e) Generation of CRL and OCSP records.
3. Security events, including:
 - a) Successful and unsuccessful attempts to access the PKI system;

- b) Actions performed by the PKI and security systems;
- c) Changes in the protection profile;
- d) Installation, update and removal of system software;
- e) System failures, hardware failures and other anomalies;
- f) Firewall and router activities; and
- g) Entering and leaving Evrotrust offices;
- h) Entering and leaving Evrotrust high security areas.

The journal entries include the following items:

1. Date and time of the record;
2. Identity of the person making the record in the journal; and
3. Description of the record.

7.4.2 KEEPING JOURNALS

Evrotrust keeps the audit journals for at least two years. The records include:

1. Evrotrust operational certificates and records of events related to the management of their life cycle:
 - a) destruction of the private key of operational certificates; or
 - b) suspension or termination of an operational certificate.
2. Records of events related to user certificate lifecycle management after suspension or termination of certificates;
3. All security event records.

7.4.3 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.

Evrotrust Information Security Plan includes an annual risk assessment that:

1. Identifies foreseeable internal and external threats that may lead to unauthorized access, disclosure, misuse, alteration or destruction of any certificate data or certificate

management processes;

2. Assesses the likelihood and potential damage from such threats, taking into account the sensitivity of certificate data or certificate management processes; and

3. Assesses whether the policies, procedures, information systems, technologies and other arrangements that Evrotrust has to counter such threats are sufficient.

7.5 ARCHIVING

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

Evrotrust keeps all documentation related to certificate applications and verification, as well as all certificates and their termination activities, for a period of 10 (ten) years after each certificate, based on such documentation, ceases to be valid.

7.6 COMPROMISE AND DISASTER RECOVERY

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

Evrotrust has developed and approved an Incident Response Plan and a Disaster Recovery Plan.

Evrotrust documents business continuity and disaster recovery procedures designed to notify and reasonably protect application software providers, users and relying parties in the event of disaster, compromise or any other business failure. These procedures are internal to the company, however, it may make them available to validators upon request. Evrotrust annually tests, reviews and updates these procedures.

The business continuity plan includes:

- a. The conditions for activating the plan,
- b. Emergency procedures,
2. Backup procedures,
3. Recovery procedures,
4. Plan support schedule;
5. Awareness and education requirements;

6. Responsibilities of the persons;
7. Recovery time objective (RTO);
8. Regular testing of contingency plans.
9. The plan maintains or restores Evrotrust's business operations in a timely manner following an interruption or failure of critical business processes;
10. Requirement for the storage of critical cryptographic materials in an alternative place;
11. What an acceptable system shutdown and recovery time is;
12. How often backups of core business information and software are made;
13. The distance of the rehabilitation facilities to the main site of Evrotrust; and
14. Procedures for safeguarding the equipment, as far as possible, during the post-disaster period and before the restoration of a safe environment of either the original or a remote site.

7.7 TERMINATION OF THE EVROTRUST ACTIVITY

7.7.1 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".

7.7.2 TRANSFER OF OPERATION TO ANOTHER PROVIDER OF QUALIFIED TRUST SERVICES

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

7.7.3 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".

8 MANAGEMENT AND CONTROL OVER THE TECHNICAL SECURITY

8.1 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".

Services".

To generate a key pair of the Certification Authority (for either a basic or an operational certificate), the following procedure shall be performed:

1. A key generation script shall be developed and followed,
2. A qualified auditor shall be ensured to witness the key pair generation process or a video of the entire generation process shall be recorded, and
3. A report shall be made stating that Evrotrust has followed its key ceremony during the key and certificate generation process and has complied with the controls used to ensure the integrity and confidentiality of the key pair.

The following requirements shall be fulfilled during the generation procedure:

1. The generation of the key pair shall be performed in a physically protected environment;
2. Officers with Trusted Roles shall participate in the key pair generation process according to the control and division of knowledge procedures;
3. The key pair generation shall be performed in cryptographic modules meeting the applicable technical and business requirements;
4. The key pair generation activities shall be documented; and
5. Effective control shall be maintained during the procedure to ensure reasonable assurance that the private key has been generated and protected in accordance with the procedures described in the applicable Policy and/or Practice and (where applicable) on the key generation script.

8.1.1 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".

8.1.1.1 REMOTE KEY PAIR GENERATION

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

Services".

8.1.2 DELIVERY OF A PRIVATE KEY TO A USER

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

8.1.3 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".

8.1.4 KEY LENGTH

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

8.1.5 PUBLIC KEY PARAMETERS

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

8.2 PROTECTION OF A PRIVATE KEY AND CRYPTOGRAPHY MODULE CONTROL

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

8.2.1 CONTROL OVER THE USE AND STORAGE OF A PRIVATE KEY

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

8.2.2 SORAGE OF A PRIVATE KEY

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

8.2.3 METHOD FOR ACTIVATION OF A PRIVATE KEY

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

Services".

8.2.4 METHOD FOR DEACTIVATION OF A PRIVATE KEY

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

8.2.5 METHOD FOR DESTRUCTION OF A PRIVATE KEY

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

8.3 OTHER ASPECTS OF MANAGING A KEY PAIR

8.3.1 PUBLIC KEY ARCHIVING

The public keys of users are contained in the Qualified Certificates issued to them, which are published in the register of certificates on Evrotrust.

8.3.2 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.

The period of use of certificates shall not exceed **397 days** and the period of validity shall not exceed **398 days**.

The evidence collected may be re-used to confirm the applicant's identity depending on the applicable law and whether the evidence is still valid given the time elapsed.

8.4 DATA FOR ACTIVATION

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

8.4.1 GENERATION AND INSTALLATION OF DATA FOR ACTIVATION

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

8.4.2 PROTECTION OF DATA FOR ACTIVATION

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

8.5 SECURITY OF COMPUTER SYSTEMS

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

8.6 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.

8.7 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.

9 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 the case of the issuance of an individual certificate;
- ETSI EN 319 412-3 in the case of the 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.

9.1 PROFILE OF A QUALIFIED ORGANIZATION WEBSITE CERTIFICATE OF AUTHENTICITY „EVROTRUST SSL ORGANIZATION VALIDATED CERTIFICATE“

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

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	[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. Specifies a general context in which other attributes of Subject field are to be understood.
	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.
	OU ¹ = (organizationalUnitName)	Organizational unit name
	2.5.4.97 ¹ = (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: <ul style="list-style-type: none"> VARBG-123456789 - VAT; NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity.
	ST ¹ = (stateOrProvinceName)	Legal entity region/state
	L ¹ = (localityName)	Legal entity locality/citi
Public Key Type/Length	RSA (2048 / 3072/ 4096 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=0.4.0.2042.1.7 [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.4.2 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)

9.2 PROFILE OF A QUALIFIED CERTIFICATE FOR AUTHENTICITY OF WEBSITE WITH EXTENDED VALIDATION „EVROTRUST SSL EV CERTIFICATE“

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

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	[UTC start date and time of certificate validity]	
Valid to	[UTC end date and time of certificate validity]	
Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Domain name, IP or Resource name

	O ⁱ = (organizationName)	Name of the legal entity: Full name under the registration or act of registration of the legal entity.
	2.5.4.97 ⁱ = (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: <ul style="list-style-type: none"> • VARBG-123456789 - VAT; • NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity.
Public Key Type/Length	RSA (2048 / 3072/ 4096 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=1.3.6.1.4.1.47272.2.5 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4	
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)	

QCStatements	id-qcs-pkixQCSyntax-v2 ⁱ (oid=1.3.6.1.5.5.7.1.1.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	id-etsi-qcs- QcLimitValue ⁱⁱ (oid=0.4.0.1862.1.2)	[Amount in BGN or EUR]
	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

9.3 PROFILE OF A QUALIFIED CERTIFICATE FOR AUTHENTICITY OF WEBSITE

„EVROTRUST SSL PSD2 CERTIFICATE“

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

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	[UTC start date and time of certificate validity]	
Valid to	[UTC end date and time of certificate validity]	
Subject	C= (countryName)	Country: Two-letter country code according to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Legal entity/organisation name:

	O ⁱ = (organizationName)	Legal entity/organisation name: Full name under the registration or act of registration of the legal entity.
	2.5.4.97 ⁱ = (organizationIdentifier)	Legal entity identifier (ETSI EN 319 412-1 p.5.1.4), for example: <ul style="list-style-type: none"> • VARBG-123456789 - VAT; • NTRBG-123456789 - UIC (BULSTAT). Enter the national identifier according to the local law of the legal entity.
Public Key Type/Length	RSA (2048 / 3072 / 4096 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	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	
Subject Alternative Name	DNS Name=[Domain name or IP]	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.2.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.194112.1.4	
Key Usage (critical)	Digital Signature (Bit 0), Key Encipherment (Bit 2)	

QCStatements	id-qcs-pkixQCSyntax-v2 (oid=1.3.6.1.5.5.7.11.2)	id-etsi-qcs-SemanticsId- Legal (oid=0.4.0.194121.1.2)
	id-etsi-qcs- QcCompliance (oid=0.4.0.1862.1.1)	
	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
	id-etsi- psd2 -qcStatement (oid=0.4.0.19495.2)	rolesOfPSP roleOfPspOid = 0.4.0.19495.1.1/2/3/4 roleOfPspName = PSP_AS/PSP_PI/PSP_AI/PSP_IC nCAName= Full name of the NCA nCAlid= NCA abbreviated unique identifier

9.4 PROFILE OF QUALIFIED CERTIFICATE FOR DOMAIN WEBSITE AUTHORITY „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	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. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Domain name, IP or Resource name
Public Key Type/Length	RSA (2048 / 3072/ 4096 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	[1]CRL Distribution Point	

Points	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)

9.5 PROFILE OF THE CERTIFICATE REVOCATION LIST (CRL)

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

9.6 OCSP / ONLINE CERTIFICATE STATUS PROTOCOL

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

10 AUDIT

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

Evrotrust periodically audits its activities by an independent external auditor. The audit verifies the compliance of Evrotrust's activities with Regulation (EU) No. 910/2014.

10.1 FREQUENCY OF THE AUDIT

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

10.2 QUALIFICATION OF THE AUDITORS

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

10.3 RELATIONSHIPS OF THE AUDITORS WITH THE PROVIDER

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

10.4 SCOPE OF THE AUDIT

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

10.5 ACTIONS TAKEN AS A RESULT OF AUDIT

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

10.6 STORAGE OF AUDIT RESULTS

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

11 OTHER BUSINESS AND LEGAL ISSUES

11.1 PRICES AND FEES

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

11.1.1 REMUNERATION

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

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

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

11.1.3 INVOICING

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

11.1.4 RETURN OF A CERTIFICATE AND RECOVERY OF PAYMENT

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

11.1.5 FREE SERVICES

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

11.2 FINANCIAL RESPONSIBILITIES

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

11.2.1 INSURANCE OF THE BUSINESS ACTIVITY

Evrotrust concludes compulsory insurance of its activity as a registered provider of Qualified Trust Services.

11.2.2 INSURANCE COVERAGE

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

11.3 CONFIDENTIALITY OF BUSINESS INFORMATION

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

Services".

11.3.1 SCOPE OF CONFIDENTIAL INFORMATION

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

11.3.2 NON-CONFIDENTIAL INFORMATION

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

11.3.3 PROTECTION OF CONFIDENTIAL INFORMATION

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

11.4 PERSONAL DATA PRIVACY

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

11.5 INTELLECTUAL PROPERTY RIGHTS

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

11.5.1 PRIVACY POLICY

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

11.5.2 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.

11.5.3 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.

11.5.4 RESPONSIBILITY FOR PROTECTION OF PERSONAL DATA

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

11.5.5 CONSENT TO USE PERSONAL DATA

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

11.6 INTELLECTUAL PROPERTY RIGHTS

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

11.6.1 DATA PROPERTY RIGHTS IN QUALIFIED CERTIFICATES

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

11.6.2 PROPERTY RIGHTS OF NAMES AND TRADE MARKS

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

11.6.3 PROPERTY RIGHTS OF A KEY PAIR

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

11.7 GENERAL

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

11.7.1 OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF EVROTRUST

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

Evrotrust gives warranties regarding the certification service provision to the following certificate beneficiaries:

1. A user who is a party to a Contract or General Terms and Conditions for the use of certificates;
2. All application software providers with which a Root CA has entered into an agreement to include its base certificate in software distributed by such provider; and
3. All relying parties who rely on a valid certificate. Evrotrust warrants to certificate beneficiaries that during the certificates' validity period, Evrotrust has complied with all requirements of its Policy and Practice.

When issuing certificates, Evrotrust is responsible for the compliance of the service with all requirements of this document and gives warranties that include, but are not limited to, the following:

1. The right to use a Domain Name or an IP address: that at the time of issuing the certificate, Evrotrust:
 - a) has applied a procedure for verification that the applicant was entitled to use, or had control of, the Domain Name and IP address(es) listed in the subject field of the certificate and the subjectAltName extension, or such right has been delegated to someone;
 - b) follows the certificate issue procedure; and
 - c) accurately describes the procedure applied in its Policy and/or Practice;
2. Authorization for a certificate: that at the time of issuing the certificate, Evrotrust:
 - a. has applied a procedure for verification that the subject authorized the issuance of the certificate and that the applicant's representative was authorized to request the certificate on behalf of the subject;
 - b. follows the certificate issue procedure; and
 - c. has accurately described the procedure applied in its Policy and/or Practice;
3. Accuracy of information: that at the time of issuing the certificate, Evrotrust:

- a. has applied a procedure for verification of the accuracy of all information contained in the certificate (except for the subject attribute: organizationalUnitName attribute);
 - b. follows the certificate issue procedure; and
 - c. has accurately described the procedure applied in its Policy and/or Practice;
- 4. No misleading information: that at the time of issuing the certificate, Evrotrust:
 - a) has applied a procedure for reducing the likelihood that the information contained in the subject attribute: organizationUnitName of the certificate is misleading;
 - b) follows the certificate issue procedure; and
 - c) has accurately described the procedure applied in its Policy and/or Practice;
- 5. Applicant's identity: that, if the certificate contains information about the subject's identity, Evrotrust:
 - a) has applied a procedure for verification of the applicant's identity in accordance with this document;
 - b) follows the certificate issue procedure; and
 - c) accurately describes the procedure applied in its Policy and/or Practice;
- 6. User Agreement (Contract): that Evrotrust and the user (Subscriber) are parties to a legally valid and enforceable agreement;
- 7. Status: Evrotrust keeps a publicly accessible 24x7 repository with up-to-date information on the status (valid or terminated) of all unexpired certificates; and
- 8. Termination: Evrotrust will terminate a certificate for any of the reasons set out in this document.

11.7.2 OBLIGATIONS, RESPONSIBILITIES AND GUARANTEES OF REGISTRATION AUTHORITY

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

11.7.3 OBLIGATIONS OF USERS

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

11.7.4 DUE CARE OF A RELYING PARTY

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

11.7.5 OBLIGATIONS OF OTHER PARTIES

11.7.5.1 OBLIGATIONS OF THE QUALIFIED VALIDATION AUTHORITY

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

11.7.5.2 OBLIGATIONS OF THE QUALIFIED OPERATIONAL CERTIFICATION AUTHORITY

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

11.7.5.3 OBLIGATIONS OF EVROTRUST TO THE PUBLIC REGISTERS/REPOSITORY

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

11.8 DISCLAIMER

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

11.9 LIMITATIONS OF RESPONSIBILITY

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

11.10 RESPONSIBILITY OF A NATURAL PERSON/LEGAL ENTITY

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

11.10.1 RESPONSIBILITY OF A NATURAL PERSON/LEGAL ENTITY TO EVROTRUST

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

11.11 DURATION AND TERMINATION OF "CERTIFICATE POLICY FOR QUALIFIED CERTIFICATION SERVICES FOR WEBSITE AUTHENTICATION"**11.11.1 DURATION**

This policy shall enter into force upon its approval by the Board of Directors of Evrotrust and its publication in the 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.

11.11.2 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.

11.11.3 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.

11.12 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.

11.13 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.

11.14 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, 1766

Okolovrasten pat 251G, Business center MM, floor 5

Telephone, Fax: + 359 2 448 58 58

email: office@evrotrust.com

Complaints will be dealt with by the legal department of Evrotrust. The complainant will receive a reply within 7 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.

11.15 APPLICABLE LAW

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

11.16 COMPLIANCE WITH THE APPLICABLE LAW

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

11.17 OTHER PROVISIONS

The policy does not specify any other provisions.

11.18 COMPLIANCE WITH STANDARDS AND STANDARDIZATION DOCUMENTS:

Evrotrust ensures that it provides certification services in accordance with all standards and standardization documents related to its scope of activity.

This document has been published on Evrotrust's website on the internet in Bulgarian and in English language. In case of any discrepancy between the Bulgarian and the English text, the Bulgarian text takes precedence.