eVrotrust

ISO/IEC 27001:2022
ISO/IEC 27701:2019
ISO 22301:2019
ISO 20000-1:2018 ISO 9001:2015
Regulation (EU) 910/2014
Regulation (EU) 2016/679

POLICY

FOR NON-QUALIFIED CERTIFICATION SERVICES

FOR ADVANCED ELECTRONIC SIGNATURE / SEAL

CONTENTS

1 INTRODUCTION

"Policy for non-qualified certification services for advanced electronic signature/seal" (the "Policy") of "Evrotrust Technologies" AD ("Evrotrust", the "Provider") defines the rules under which Evrotrust issues and manages non-qualified certificates supporting advanced electronic signatures within the meaning of Article 26 and advanced electronic seals within the meaning of Article 36 of Regulation (EU) No 910/2014 ("eIDAS").

Evrotrust is a qualified trust service provider under Regulation (EU) No 910/2014, supervised by the Communications Regulation Commission (CRC) of the Republic of Bulgaria. The services governed by this Policy are, however, NOT qualified trust services. This Policy is deliberately drafted as a lean, reference-based document: matters not expressly regulated herein are governed by the "Practice Statement for Non-Qualified Trust Services" (eIDAS-CPS-NQ) and, through it, by the "Certification Practice Statement" of Evrotrust (eIDAS-CPS), as published on https://evrotrust.com/tsp-documents/, applied mutatis mutandis to non-qualified certificates. The

certificates governed by this Policy correspond to the non-qualified certificate for advanced electronic signature regulated in item 2.2 of the General Terms and Conditions ("GTC") and the corresponding non-qualified certificate profiles for advanced electronic seal, together with any short-term certificates issued for one-time signing in connection with the non-qualified service for management of remote signature/seal creation devices under item 2.4.2 of the GTC.

1.1 STATUS OF THE SERVICE – IMPORTANT NOTICE

For the avoidance of any doubt, in respect of the services under this Policy:

- the services are not included in the Bulgarian Trusted List under Article 22 of Regulation (EU) No 910/2014 and do not carry the EU trust mark (Article 23);
- certificates issued to natural persons under this Policy are not qualified certificates for electronic signatures within the meaning of Article 3(15) and Annex I of Regulation (EU) No 910/2014;
- certificates issued to legal persons under this Policy are not qualified certificates for electronic seals within the meaning of Article 3(30) and Annex III of Regulation (EU) No 910/2014;
- electronic signatures created with certificates governed by this Policy do not have the legal effect equivalent to that of handwritten signatures provided for qualified electronic signatures under Article 25(2) of Regulation (EU) No 910/2014;
- electronic seals created with certificates governed by this Policy do not benefit from the presumption of integrity of the data and correctness of the origin of the data provided for qualified electronic seals under Article 35(2) of Regulation (EU) No 910/2014;
- no qualified signature/seal creation device (QSCD) is required or asserted;
- pursuant to Articles 25(1) and 35(1) of Regulation (EU) No 910/2014, an electronic signature or electronic seal shall not be denied legal effect or admissibility as evidence in legal proceedings solely because it is in electronic form or because it does not meet the requirements for qualified electronic signatures or qualified electronic seals.

1.2 COMPLIANCE

This Policy is structured with regard to IETF RFC 3647 and follows the requirements of the

Lightweight Certificate Policy (LCP) defined in ETSI EN 319 411-1, building on the general policy requirements of ETSI EN 319 401. The collection and validation of identity attributes and identity evidence is guided by ETSI TS 119 461, clauses 8.2, 8.3 and, as applicable to the agreed binding practices, clause 8.4, as further specified in section 3 of this Policy. Certificate content follows ETSI EN 319 412 (without qualified certificate statements). This Policy incorporates, without restating them, all requirements of ETSI EN 319 411-1 applicable at LCP level that carry no policy-specific marking (OVR-7.1-09), as implemented through the Practice Statement for Non-Qualified Trust Services and the Certification Practice Statement; the identifiers in section 1.3 implement OVR-7.1-02 and OVR-7.1-12. The selection of the LCP policy level is supported by a documented risk assessment (ETSI EN 319 411-1, clauses 4.2.2 and 7.1, OVR-7.1-04). Baseline LoIP identifies the assurance level of the identity-proofing process and does not change the certificate-policy level from LCP to NCP. A use case requiring compliance with the NCP policy shall be governed by a separate certificate policy containing the applicable NCP policy identifier.

As a non-qualified trust service provider in respect of the services hereunder, Evrotrust complies with Article 13 (liability) and Article 19a (requirements for non-qualified trust service providers) of Regulation (EU) No 910/2014, with the Bulgarian Electronic Document and Electronic Trust Services Act, and with the Ordinance on the liability and termination of the activity of providers of certification services (adopted by CMD No 176/2018), including the minimum insurance requirement thereunder.

1.3 NAME AND IDENTIFIER OF THE POLICY

This document is entitled "Policy for non-qualified certification services for advanced electronic signature/seal". The certificates issued hereunder contain the following policy identifiers, registered in the Evrotrust OID register (SF 18.1.1.3):

Ref.	Certificate type / identity verification approach	Evrotrust OID	ETSI policy OID
Standard	Evrotrust Advanced Natural Person Certificate for AES – standard identity verification	1.3.6.1.4.1.47272.4.1.4.1	LCP – 0.4.0.2042.1.3
Baseline LoIP	Evrotrust Advanced Natural Person Certificate for AES – identity verification at Baseline LoIP	1.3.6.1.4.1.47272.4.1.4.2	LCP – 0.4.0.2042.1.3

Ref.	Certificate type / identity verification approach	Evrotrust OID	ETSI policy OID
Standard	Evrotrust Advanced Legal Person Certificate for AESeal – standard identity verification	1.3.6.1.4.1.47272.4.1.4.3	LCP – 0.4.0.2042.1.3
Baseline LoIP	Evrotrust Advanced Legal Person Certificate for AESeal – identity verification at Baseline LoIP	1.3.6.1.4.1.47272.4.1.4.4	LCP – 0.4.0.2042.1.3

The identity verification approach applied at issuance is indicated in each certificate through the corresponding Evrotrust policy identifier, so that any relying party can establish from the certificate alone which approach was applied. The LCP identifier identifies the applicable certificate-policy level. The Evrotrust policy identifier separately identifies the Subject type and the identity-verification approach applied at issuance. Baseline LoIP does not alter the LCP certificate-policy level.

In commercial and marketing materials of Evrotrust the certificates issued under this Policy may be designated "Advanced Electronic Certificate". That designation is a commercial name for the non-qualified certificates governed by this Policy and does not alter their non-qualified status, the applicable certificate-policy level, or any right or obligation set out herein.

1.4 PARTICIPANTS IN THE INFRASTRUCTURE

Non-qualified certificates under this Policy are issued by the operational certification authority "Evrotrust RSA Advanced Operational CA 2025" (the "Advanced CA"), operated within the Evrotrust infrastructure and dedicated exclusively to non-qualified certificates. The Advanced CA is separate from the operational certification authorities issuing qualified certificates. Registration services are performed by the Registration Authority of Evrotrust, by partners acting as external Registration Authorities under an agreement with Evrotrust, or, where attestation is an agreed identification method, partly relied upon from an approved Subscriber acting as an attesting source under section 3.2. In all cases Evrotrust remains responsible for the compliance of the registration services with this Policy (ETSI EN 319 411-1, OVR-5.4.1-01).

Subscribers are typically corporate clients contracting the service for their own customers or personnel; Subjects are the natural persons (or, for seals, legal persons) named in the certificates;

Relying Parties are persons acting in reliance on certificates issued hereunder. The rights and obligations of all participants are governed by the General Terms and Conditions of the contract for trust, information, cryptographic and other services of Evrotrust, the applicable Tariff, and the subscriber agreement.

1.5 POLICY MANAGEMENT

1.5.1 POLICY MANAGEMENT ORGANIZATION

Evrotrust is responsible for the management of this Policy. Each version of this Policy is in force until the approval and publication of a new version. Each new version is developed by employees of Evrotrust and is published after approval by the Board of Directors of Evrotrust, which is the body with final authority and responsibility for specifying and approving this Policy (ETSI EN 319 411-1, OVR-7.1-03).

Subscribers, Subjects and Relying Parties are required to comply only with the version of this Policy in force at the time the services are used.

This Policy is reviewed at least annually, and upon material change of the applicable standards or legislation, under a defined review process which ensures that it remains supported by the Practice Statement for Non-Qualified Trust Services (OVR-7.1-05, OVR-7.1-06). Amendments are published on the Evrotrust website.

1.5.2 CONTACT PERSON

The contact person for the management of this Policy is the Executive Director of Evrotrust Technologies AD. Further information can be obtained at the following address:

Evrotrust Technologies AD, 251G Okolovrasten pat Str., MM Business Center, fl. 5, 1766 Sofia, Bulgaria; office@evrotrust.com; +359 2 448 58 58; https://www.evrotrust.com.

1.5.3 RELATIONSHIP BETWEEN POLICY AND PRACTICE

This Policy and the Practice Statement for Non-Qualified Trust Services (eIDAS-CPS-NQ) cover the same subject matter from different perspectives. This Policy states the requirements applicable to the issuance and management of non-qualified certificates and identifies the participants in the provision of the services, while the Practice Statement states how Evrotrust and the other participants in its infrastructure apply the procedures and controls that meet those requirements. A single practice statement may support several policies used for different applications or with a different scope for different Relying Parties.

1.5.4 CONTACT PERSON AND PRACTICE APPROVAL PROCEDURES

The person who takes decisions on the performance of the Practice Statement for Non-Qualified Trust Services (eIDAS-CPS-NQ) and is responsible for its management is the Executive Director of Evrotrust Technologies AD. The Practice Statement for Non-Qualified Trust Services is developed by employees of Evrotrust and is approved by the Board of Directors of Evrotrust. Each version is in force until the approval and publication of a new version.

2 IDENTITY VERIFICATION APPROACHES

All certificates under this Policy are issued at the LCP policy level of ETSI EN 319 411-1. Evrotrust does not define a single rigid identification flow: in line with item 6.3.1.1 of the GTC, the identification methods applicable to each subscriber arrangement are agreed and documented through the "Client Identification Practices Questionnaire", assessed and approved by the Information Security Management Commission (ISMC) under SP A.06 Organization of information security, and implemented through the agreement with the client. Two identity verification approaches are distinguished, indicated in each certificate by the policy identifiers under section 1.3:

- Standard identity verification (default): collection and validation of identity attributes and evidence guided by ETSI TS 119 461, clauses 8.2 and 8.3, through the methods agreed per arrangement (for example, submission of evidence, attestation from an appropriate and authorized source, identification by a partner acting as an external Registration Authority, or reuse of a prior identification), with identity binding measures as agreed - no level of identity proofing (LoIP) is claimed;
- Identity verification at Baseline LoIP (where contractually agreed): for a natural-person Subject, identity proofing is performed at Baseline Level of Identity Proofing in accordance with ETSI TS 119 461, including the applicable requirements of clauses 8.2, 8.3 and 8.4 and an approved natural-person use case under clause 9.2; for a legal-person Subject, identity proofing of the legal person conforms to an applicable use case under clause 9.3 and, where a natural person acts as representative of the legal person, clause 9.4 also applies, including Baseline LoIP identity proofing of the representative under an applicable use case of clause 9.2 and validation of the representative's role and authority to act for the legal person.

3 IDENTIFICATION AND VERIFICATION OF IDENTITY

3.1 GENERAL REQUIREMENTS – ALL APPROACHES

For every certificate issued under this Policy, Evrotrust collects and validates either direct evidence or an attestation from an appropriate and authorized source of the identity of the Subject and, where applicable, of any specific attributes, in accordance with ETSI EN 319 411-1, requirements REG-6.2.2-01, REG-6.2.2-02A, REG-6.2.2-02AB, REG-6.2.2-02AC and REG-6.2.2-02B. The collection of attributes and evidence and their validation are guided by ETSI TS 119 461, clauses 8.2 (attribute and evidence collection) and 8.3 (attribute and evidence validation), applied to the extent relevant to the evidence types accepted for the given subscriber arrangement.

For a natural person, evidence is collected of the full name and of the date and place of birth, a reference to a nationally recognized identity document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name (ETSI EN 319 411-1, REG-6.2.2-06 and REG-6.2.2-07).

For a legal-person Subject, evidence is collected and validated regarding at least the registered legal name, registration number or other authoritative identifier, country of establishment and active legal existence. Where a natural person acts for the legal person, the identity of that natural person and the person's authority to request the certificate or control the electronic seal are verified and recorded in accordance with the approved identity-proofing process.

In accordance with ETSI EN 319 411-1, REG-6.3.1-00C, the process used for the initial verification of the identity and the attributes of the Subject is in every case an applicable identity proofing process as per the practice statement at the time of issuing the certificate. To this end, Evrotrust maintains for every subscriber arrangement a documented identity proofing process description covering, as a minimum, the collection of identity attributes and evidence (ETSI TS 119 461, clause 8.2) and their validation (ETSI TS 119 461, clause 8.3), together with the identity binding practices applicable to the arrangement. The applicable process is agreed and documented in the course of contracting on the basis of the "Client Identification Practices Questionnaire" and is approved by the ISMC before the first issuance, the decision being recorded in the minutes of the Commission (SF 06.1.1.1).

Identity binding measures – the verification that the applicant is the person identified by the

presented evidence (ETSI TS 119 461, clause 8.4) – forms part of every identity proofing process under this Policy. Depending on the agreed process description, binding measures are executed by Evrotrust (including through the identification services referred to in section 3.3), by the Subscriber as an attesting source, and/or through compensating controls appropriate to the risk of the arrangement, such as delivery of the certificate and its activation data through a channel authenticated to the Subject. Unless identity verification at Baseline LoIP is expressly agreed, the binding practices applied do not claim conformance to a level of identity proofing (LoIP) under ETSI TS 119 461. The binding practices for each arrangement are documented in the identity proofing process description; records of the identification performed are created and retained in accordance with the Practice Statement.

3.2 STANDARD IDENTITY VERIFICATION

Under the standard approach for Subscriber Identification in the case of provision of non-qualifies services, in accordance with item 6.3.1.1 of the GTC of Evrotrust, the identity of the Subject is established through one or more of the following methods, as agreed and documented in the identity proofing process description for the subscriber arrangement:

- submission of identity evidence (an official identity document or other accepted evidence) through the agreed channel, validated by Evrotrust guided by ETSI TS 119 461, clause 8.3: acceptance of the document type and issuer, validity period, authenticity and integrity as far as practicable for the form in which the evidence is presented, and current status where an online status service is practically available;
- an attestation of identity from an appropriate and authorized source (ETSI EN 319 411-1, REG-6.2.2-02A) – typically a Subscriber, such as an employer, a financial institution or a public body, which has already identified the Subject under its own regulatory or contractual framework – validated by Evrotrust as to the authority of the source and the authenticity and integrity of the attestation (ETSI TS 119 461, clause 8.3.8);
- identification performed by a partner acting as an external Registration Authority of Evrotrust, supported by the standardized per-issuance request/declaration for issuing of a non-qualified certificate based on identification performed by an external Registration Authority, signed with a qualified electronic signature by an authorized representative of

the partner; the declaration identifies the Registration Agent who performed the identification, confirms that the identity of the Subject has been verified through physical presence or another process agreed between the parties, and records that the Subject has been informed of, and consents to, the issuance and signing process;

- reuse of an identification previously performed by Evrotrust for another of its services, where permitted by the applicable policies.

The use of attestations, and any allocation of identification steps to the Subscriber, is available only under arrangements approved in advance by the ISMC, case by case, on the basis of the completed "Client Identification Practices Questionnaire". The subscriber agreement includes in each case a warranty of the accuracy of the identity data declared or attested, the obligation to retain the underlying identification records and to make them available to Evrotrust upon request, audit rights of Evrotrust, the allocation of responsibility for identification, and termination rights in the event of breach. Identity binding is performed through the measures agreed in the identity proofing process description – such as delivery of the certificate and its activation data through a channel authenticated to the Subject, verification measures operated by the Subscriber, or binding measures executed by Evrotrust – in line with the practices of ETSI TS 119 461, clause 8.4, but without a claim to a level of identity proofing.

The applied approach is disclosed to Relying Parties through the policy identifiers under section 1.3 and the applicable terms. Relying Parties should not assume unambiguous identification of the Subject on the basis of a certificate issued under the standard approach alone. The standard approach is intended for use cases where the Relying Party or the Subscriber operates its own verification of the user, or where the risk assessment of the arrangement supports the agreed methods and binding measures.

3.3 IDENTITY VERIFICATION AT BASELINE LOIP

Where contractually agreed for a natural-person Subject, identity proofing is performed at Baseline Level of Identity Proofing in accordance with ETSI TS 119 461, with full application of clause 8.4 (binding to applicant) through an applicable natural-person use case under clause 9.2, using the identification capabilities of Evrotrust, including as applicable: the qualified at a national level service for electronic identification (eIDAS-CP-CPS-IdV); the registration authority

service for identification using remote video identification (eIDAS-CP-CPS-RA-R); the registration authority service for identification by physical presence (eIDAS-CP-CPS-RA-P); or automated remote identification through the Evrotrust mobile application as described in the Certification Practice Statement. The applicable use cases are documented per flow in the Practice Statement and the respective service policies. This approach, or individual Baseline LoIP flows within a standard arrangement, may also be agreed for a subset of Subjects.

For a legal-person Subject, the applicable Baseline LoIP requirements are those set out in sections 2 and 3.1 of this Policy, including clauses 9.3 and 9.4 of ETSI TS 119 461 and Baseline LoIP identity proofing of the representative under an applicable use case of clause 9.2.

3.4 IDENTIFICATION IN CONNECTION WITH CERTIFICATE MANAGEMENT

Identification and verification of identity upon renewal, suspension, revocation and after termination of validity of a certificate follow the corresponding provisions of the Certification Practice Statement, applied mutatis mutandis, with the clarification that re-identification for a new certificate applies the identity verification approach under which the new certificate is requested.

4 OPERATIONAL REQUIREMENTS

The operational procedures for registration, application processing, issuance, acceptance, publication, suspension, resumption, revocation and status services follow section 4 of the Certification Practice Statement, applied mutatis mutandis to non-qualified certificates, subject to the modifications listed in the Practice Statement for Non-Qualified Trust Services. For certificate profiles for which revocation status services are provided, CRL and OCSP are operated through the common Evrotrust infrastructure and at the same service levels as for qualified certificates. Revocation takes effect upon publication and no later than 24 hours after receipt of a valid request. Certificates issued under this Policy are published in a repository segment clearly designated as non-qualified. The terms and conditions applicable to a given certificate are readily identifiable through the policy identifiers referred to in section 1.3 (ETSI EN 319 411-1, DIS-6.1-05 and DIS-6.1-06A).

Before entering into a contractual relationship, Evrotrust informs the Subscriber of the applicable terms and conditions in a durable and human-readable form, which may be transmitted

electronically (ETSI EN 319 411-1, REG-6.3.4-02, OVR-6.3.4-04, OVR-6.3.4-05). The agreement with the Subscriber and, where the Subject is a separate natural or legal person, with the Subject, is recorded and involves explicit acceptance of the terms and conditions by a wilful act which can later be supported by evidence (REG-6.3.4-07, REG-6.3.4-08); where Subscriber and Subject differ, the agreement is concluded in two parts (REG-6.3.4-09 et seq.). The terms and conditions indicate what is deemed to constitute acceptance of a certificate (OVR-6.3.4-01). The agreement includes consent to the keeping by Evrotrust of records of the information used in registration and certificate management and to the passing of this information to third parties under the same conditions in the case of termination of the services (REG-6.3.4-10A), as well as consent to publication of the certificate where applicable. Registration records, agreements and certificate lifecycle records are retained for the period stated in the terms and conditions, that is ten years after the certificate based on them ceases to be valid, under applicable Bulgarian legislation, satisfying the minimum retention required by OVR-6.4.6-01.

5 KEY MANAGEMENT AND TECHNICAL CONTROLS

The keys of the Advanced CA are generated, stored and used exclusively within cryptographic modules certified to FIPS PUB 140-2 level 3 (or higher) or Common Criteria EAL 4+ in accordance with section 6 of the Certification Practice Statement, within the same secured environment, under the same dual control and trusted-role arrangements as the qualified certification authorities of Evrotrust.

Subject keys may be generated: (a) by the Subject or Subscriber, in which case possession of the private key is verified through the certificate signing request/CSR (PKCS#10); or (b) by Evrotrust in its infrastructure, in which case, where Evrotrust provides a remote signature or seal creation component and generates or manages the corresponding Subject keys, Evrotrust applies controls aligned with the applicable provisions of ETSI TS 119 431-1 without asserting use of a remote QSCD or full conformity of every service component with ETSI TS 119 431-1 so that the Subject retains sole control or, for legal persons, control over the private key, in support of Article 26(c) for advanced electronic signatures and Article 36(c) for advanced electronic seals, as applicable, of Regulation (EU) No 910/2014. No QSCD is used or claimed for Subject keys. Subject keys use algorithms, key lengths and parameters suitable for the certified key uses in accordance with ETSI

TS 119 312 as applicable at the time of issuance.

6 SIGNATURE CREATION AND VALIDATION

Where Evrotrust provides signature or seal creation, augmentation or validation as part of the applicable service, the relevant processes follow ETSI EN 319 102-1 and the applicable signature-format standards including CAdES (ETSI EN 319 122), XAdES (ETSI EN 319 132), PAdES (ETSI EN 319 142) and the associated ASiC containers (ETSI EN 319 162) for the formats and service components supported.

When the signing process using an electronic signature or electronic seal is operated by Evrotrust (item 2.4.2 of the GTC), the signing flow implements the controls of ETSI EN 319 102-1, clause 4.3.2.4: presentation of the document, or of a reliable representation of it, to the Signatory or authorized seal controller, as applicable; information on the implications of signing using an electronic signature or electronic seal and recording of the Signatory's consent or the authorized act of the seal controller expressed through a wilful act; authentication of the Signatory or authorized seal controller before activation of the signature or seal creation data; verification that the signing certificate is cryptographically correct, within its validity period and not revoked at the time of signing; and verification of the created signature or seal before its release. These controls, together with the sole-control measures under section 5, support the fulfilment of the conditions of Articles 26 and 36, as applicable, of Regulation (EU) No 910/2014.

The default signature or seal level is signature with time (B-T), applying a qualified electronic time stamp of Evrotrust; long-term levels (B-LT, B-LTA) are applied where agreed, having regard to the retention and evidentiary needs of the use case. Signature or seal creation, augmentation and validation are governed by internal signature creation, augmentation and validation policies (configurations) maintained under the Practice Statement. Validation of signatures is available through the validation services of Evrotrust in accordance with ETSI EN 319 102-1, clause 5, returning a status indication and a validation report. A technically positive validation result does not by itself determine the legal or business suitability of a signature for a particular transaction.

7 CERTIFICATE PROFILES

Certificates issued under this Policy follow ETSI EN 319 412-2 for natural persons and ETSI EN

319 412-3 for legal persons, without any qualified-certificate statements. The profiles include the issuer "Evrotrust RSA Advanced Operational CA 2025", the applicable policy identifiers under section 1.3 and the certificate fields and extensions defined in the Annex to the Practice Statement for Non-Qualified Trust Services.

KeyUsage is marked critical and is set in accordance with the applicable approved certificate profile.

Information identifying an attesting Subscriber, external Registration Authority or other evidence provider is retained in the registration records and is not encoded as an identity attribute of the certificate Subject.

Certificates governed by this Policy are non-qualified certificates and do not contain the QcStatements extension (EN 319 412-5). Consequently, no qualified-certificate statement, including QcCompliance, QcType, QcSSCD, QcPDS, QcLimitValue or an ETSI Semantics Identifier carried through QcStatements, is asserted.

8 LIABILITY AND LEGAL PROVISIONS

Evrotrust is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under Regulation (EU) No 910/2014, in accordance with Article 13(1) thereof. The burden of proving intention or negligence of Evrotrust in respect of the non-qualified services hereunder lies with the natural or legal person claiming the damage.

Evrotrust is not liable for damage arising from the use of services exceeding the limitations indicated in this Policy, in the certificate content or in the applicable terms (Article 13(2)). Liability is otherwise applied in accordance with Bulgarian law (Article 13(3)).

Evrotrust maintains the insurance (or equivalent financial resources) required under the Ordinance on the liability and termination of the activity of providers of certification services, covering also the services under this Policy.

Under the standard identity verification approach, responsibility for the identification and binding measures allocated to the Subscriber under the identity proofing process description lies with the Subscriber, as set out in the subscriber agreement and the applicable terms.

8.1 OBLIGATIONS OF SUBSCRIBERS AND SUBJECTS

In accordance with ETSI EN 319 411-1, OVR-6.3.5-01 and OVR-6.3.5-02, the terms and conditions

place on the Subscriber (and, where the Subject is a separate natural or legal person, on the Subject in respect of the items applicable to it) at minimum the following obligations:

- to provide Evrotrust with accurate and complete information at registration and to keep it up to date;
- to use the key pair only in accordance with the limitations notified to the Subscriber and the Subject, and to prevent any unauthorized use of the Subject's private key;
- where the Subscriber or the Subject generates the Subject's keys: to use algorithms and key lengths in accordance with ETSI TS 119 312 for the certified key uses, and, for signature key usages, to maintain the private key under the Subject's sole control (or, for legal persons, under the Subject's control);
- to notify Evrotrust without any reasonable delay, up to the end of the validity period of the certificate, if the Subject's private key has been lost, stolen or potentially compromised, if control over the private key has been lost due to compromise of activation data or otherwise, or in the event of inaccuracy of or changes to the certificate content;
- following compromise of the private key, to immediately and permanently discontinue its use, except for key decipherment;
- upon being informed that the certificate has been revoked or that the issuing CA has been compromised, to ensure that the private key is no longer used by the Subject.

8.2 NOTICE TO RELYING PARTIES

In accordance with ETSI EN 319 411-1, OVR-6.3.5-03, Relying Parties are recommended, before relying on a certificate issued under this Policy, to: verify, where applicable to the certificate profile, the validity, suspension or revocation status of the certificate using the current revocation status information (CRL/OCSP); take account of the identity verification approach indicated by the policy identifiers and of any limitations on the usage of the certificate indicated in the certificate or in the applicable terms; and take any other precautions prescribed in agreements or elsewhere.

8.3 LIMITATIONS OF USE AND LIABILITY

Certificates issued under this Policy are intended solely for the creation of advanced electronic signatures and advanced electronic seals, in accordance with the KeyUsage and any applicable

ExtendedKeyUsage indicated in the certificate. Any other use is outside the intended purpose of the certificates and takes place at the sole risk of the user.

Any transaction-value or reliance limit applicable to a certificate or service governed by this Policy is stated in the applicable PKI Disclosure Statement, Subscriber agreement or service-specific notice. Such limitation is not represented in the certificate through QcStatements. Refunds upon termination of the service are governed by the General Terms and Conditions and the Tariff.

Evrotrust shall not be held liable for damages caused by:

- the use of a certificate outside the scope of its intended purposes and the limitations indicated in it, in this Policy or in the applicable terms, including the reliance limit;
- unlawful actions of the Subscriber, the Subject or the Relying Party, or failure of a Relying Party to perform the verifications recommended in section 8.2;
- reliance on the identity in a certificate beyond the scope of the identity verification approach indicated by its policy identifiers, including reliance on a certificate issued under the standard approach as unambiguous identification of the Subject;
- inaccuracy of identity data declared or attested by the Subscriber or the declaring person, responsibility for which lies with that person as provided in item 6.3.1.1 of the GTC and allocated in the subscriber agreement;
- provision of the means of access to the private key or its activation data by the Subject to third parties, or compromise of the private key at the fault of the Subject;
- use of a certificate that has not been issued or used in accordance with this Policy and the Practice Statement, or use of a suspended, revoked or expired certificate;
- untimely action to revoke or suspend a certificate for reasons beyond the control of Evrotrust;
- incidental events of the nature of force majeure, including malicious actions of third parties;
- poor quality or functionality of software products and hardware devices used by the Subscriber, the Subject or the Relying Parties.

The limitations under this section apply to the maximum extent permitted by applicable law and do not exclude or limit any liability which cannot be excluded or limited under Bulgarian law, nor do they derogate from the insurance maintained under the Ordinance referred to in section 1.2. The limitations are indicated in advance to Subscribers and Subjects through the terms and

conditions and are recognisable to third parties through the policy identifiers in the certificates, this Policy and the PKI disclosure statement published on the Evrotrust website (Article 13(2) of Regulation (EU) No 910/2014).

8.4 TERMS AND CONDITIONS AND PKI DISCLOSURE STATEMENT

The terms and conditions applicable to the services hereunder comprise the General Terms and Conditions, this Policy and the subscriber agreement. They include, at minimum, the elements required by ETSI EN 319 411-1, OVR-6.9.4-02: the indication of what constitutes certificate acceptance; the retention period of the registration records; the obligations of Subscribers and Subjects; the notice to Relying Parties; and the ways in which this Policy adds to or further constrains the requirements of the LCP certificate policy (OVR-7.2-01).

Evrotrust publishes a PKI disclosure statement for the service (eIDAS-PDS-NQC-AES) following the model in Annex A of ETSI EN 319 411-1. The General Terms and Conditions of the contract for trust, information, cryptographic and other services, the Privacy Policy applicable to the services of Evrotrust and the applicable Tariff apply to the services under this Policy.

This document has been published on Evrotrust's website on the internet in English language.