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

PRACTICE STATEMENT

FOR NON-QUALIFIED TRUST SERVICES

CONTENTS

1 INTRODUCTION....3
1.1 DRAFTING TECHNIQUE – INCORPORATION BY REFERENCE....3
2 APPLICABILITY OF THE MAIN CPS....4
3 MODIFICATIONS....5
4 FUTURE NON-QUALIFIED SERVICES....9
5 ANNEX: CERTIFICATE, CRL AND OCSP PROFILES....9
5.1 PROFILE OF OPERATIONAL CERTIFYING AUTHORITY „EVROTRUST RSA ADVANCED OPERATIONAL CA 2025“....9
5.2 PROFILE OF OCSP RESPONDER „EVROTRUST RSA ADVANCED OPERATIONAL CA 2025 OCSP”....11
5.3 PROFILE OF THE CRL OPERATIONAL CERTIFICATION AUTHORITY „EVROTRUST RSA ADVANCED 2025“....12
5.4 PROFILE OF A NON-QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE OF A NATURAL PERSON "EVROTRUST ADVANCED NATURAL PERSON CERTIFICATE FOR AES – STANDARD"....12
5.5 PROFILE OF A NON-QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE OF A NATURAL PERSON "EVROTRUST ADVANCED NATURAL PERSON CERTIFICATE FOR AES – BASELINE LOIP"....15
5.6 PROFILE OF A NON-QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SEAL OF A LEGAL PERSON “EVROTRUST ADVANCED LEGAL PERSON CERTIFICATE FOR AESEAL – STANDARD”....17
5.7 PROFILE OF A NON-QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SEAL OF A LEGAL PERSON “EVROTRUST ADVANCED LEGAL PERSON CERTIFICATE FOR AESEAL – BASELINE LOIP”....18
6 FINAL PROVISIONS....20

1 INTRODUCTION

This "Practice Statement for Non-Qualified Trust Services" (the "Practice Statement", eIDAS-CPS-NQ) states the practices applied by "Evrotrust Technologies" AD ("Evrotrust") in the provision of trust services which are not qualified trust services within the meaning of Regulation (EU) No 910/2014. It currently applies to the issuance and management of non-qualified certificates for advanced electronic signature/seal under the "Policy for non-qualified certification services for advanced electronic signature/seal" (eIDAS-CP-NQC-AES).

This Practice Statement is designed as an umbrella document for all present and future non-qualified trust services of Evrotrust. Future services (including, when applicable standards are adopted, services related to electronic attestations of attributes) will be accommodated by adding service-specific annexes, without amendment of the core of this document.

1.1 DRAFTING TECHNIQUE – INCORPORATION BY REFERENCE

Evrotrust provides the non-qualified services using the organization, personnel, facilities, information security management system and technical infrastructure described in the current published version of the "Certification Practice Statement for Qualified Trust Services" of Evrotrust, document identifier eIDAS-CPS, available in the Evrotrust repository at https://evrotrust.com/tsp-documents (the "Main CPS"). Unless expressly modified or excluded by this Practice Statement, each new version of the Main CPS becomes applicable to the non-qualified services upon its publication. For the purposes of determining the practices applicable to a particular certificate lifecycle event, the applicable version of the Main CPS is the version published and in force at the time of that event. In the event of conflict, this Practice Statement and the applicable certificate policy prevail in respect of the non-qualified services.

To avoid duplication, this Practice Statement incorporates the Main CPS by reference, section by section, with one of the following dispositions:

- "Applies" – the referenced section of the Main CPS applies to the non-qualified services mutatis mutandis; references therein to "qualified certificate(s)" are read as "non-qualified certificate(s)" and references to the qualified operational certification authorities are read as references to "Evrotrust RSA Advanced Operational CA 2025";
- "Modified" – the referenced section applies subject to the modifications set out in section 3 of this Practice Statement;
- "Not applicable" – the referenced section concerns exclusively qualified trust services and

does not apply.

The mutatis mutandis reading rule does not extend to provisions whose applicability depends on qualified status, inclusion of a service in the Trusted List as a qualified service, use of the EU trust mark, use or assertion of a QSCD, inclusion of QcStatements, or conformity assessment under Article 20 of Regulation (EU) No 910/2014. Such provisions apply to the non-qualified services only where expressly restated in this Practice Statement or the applicable certificate policy.

2 APPLICABILITY OF THE MAIN CPS

Main CPS section	Disposition	Notes
1. Introduction, participants, hierarchy	Modified	**M1:** the Advanced CA hierarchy for the non-qualified services is defined in this Practice Statement; participants are defined in eIDAS-CP-NQC-AES.
2. Publication and repository	Modified	**M3:** non-qualified certificates published in a clearly designated repository segment; same availability infrastructure.
3. Identification and verification of identity	Modified	**M2:** identification per section 3 of eIDAS-CP-NQC-AES (standard / Baseline LoIP approaches); assessment and approval by the Information Security Management Commission (ISMC) under SP A.06 apply.
4.1–4.8 Certificate application, issuance, acceptance, key pair update	Applies	Mutatis mutandis; channels per subscriber agreement.
4.9 Suspension and revocation	Applies	Same grounds, procedures and time limits (revocation ≤ 24 h after valid request; REV-6.2.4-03A), incl. the exception procedures of the Main CPS where a revocation request cannot be confirmed within 24 h (REV-6.2.4-03BA).
4.10 Certificate status services (CRL/OCSP)	Modified	The common infrastructure and service levels apply to certificate profiles for which CRL or OCSP status services are provided. The service-specific status model is defined in the Annex.
5. Facility, management and operational controls (incl. trusted roles, records, archival, incident management, business continuity, termination)	Applies	Same premises, roles, event logging, archival and continuity arrangements; termination plan covers the non-qualified services; see **M7** for records of identification.
6. Technical security controls (CA key generation and	Applies	The cryptographic module and certification applicable to each Advanced CA, OCSP responder and centrally managed Subject-key component are specified in the

Main CPS section	Disposition	Notes
protection, cryptographic modules, activation data, computer and network security)		applicable approved component configuration; the common dual-control, trusted-role, system-security and lifecycle controls of Main CPS section 6 apply.
7. Certificate, CRL and OCSP profiles	Modified	**M4:** profiles per eIDAS-CP-NQC-AES section 7 and the Annex hereto; no QcStatements.
8. Compliance audit and other assessment	Modified	**M6:** no conformity assessment under Art. 20 eIDAS is required for the non-qualified services; internal audits and ISO 9001/27001/20000-1/22301 certifications cover them; voluntary notification to the CRC may be made.
9. Other business and legal matters (fees, confidentiality, personal data, liability, term and termination, dispute resolution, governing law)	Modified	**M8:** liability per Art. 13 eIDAS and the national Ordinance (insurance); GTC, Privacy Policy and Tariff apply; allocation of identification responsibility per subscriber agreements; **M10**: reliance limits and waiver grounds for non-qualified certificates.
10. Terms and abbreviations	Applies	Supplemented with the terms defined in eIDAS-CP-NQC-AES.

3 MODIFICATIONS

M1 (Hierarchy)

- The operational certification authority "Evrotrust RSA Advanced Operational CA 2025" is established within the Evrotrust hierarchy and is dedicated exclusively to non-qualified certificates. For the non-qualified services governed by this Practice Statement, this section and the applicable Annex constitute the authoritative description of the Advanced CA hierarchy. The certification path for end-user certificates governed by this Practice Statement is:
  - Root CA is "Evrotrust RSA Root CA";
  - Intermediate CA is "Evrotrust Intermediate CA";
  - Operational CA is "Evrotrust RSA Advanced Operational CA 2025";
  - End-user certificate.

  The OCSP responder certificate for this hierarchy is issued by "Evrotrust RSA Advanced Operational CA 2025" and is used solely for status information relating to the applicable non-qualified certificate profiles. The certification path and the CA certificates of this

hierarchy are published in the Evrotrust repository. Its key ceremonies, key protection and lifecycle follow section 6 of the Main CPS.

M2 (Identification)

- For every subscriber arrangement, an identity proofing process description is documented and approved by the ISMC under SP A.06 Organization of information security before the first issuance (ETSI EN 319 411-1, REG-6.3.1-00C). Each process covers, as a minimum, the collection and validation of identity attributes and evidence (ETSI TS 119 461, clauses 8.2 and 8.3) and defines the identity binding practices applied, which may be executed by Evrotrust (including through its identification services), by the subscriber as an attesting source, or jointly, with compensating controls as assessed. Except where identity verification at Baseline LoIP is agreed, no level of identity proofing under ETSI TS 119 461 is claimed. For a Baseline LoIP natural-person profile, the applicable use case under clause 9.2 of ETSI TS 119 461 is identified in the approved process description. For a Baseline LoIP legal-person profile, the applicable legal-person use case under clause 9.3 is identified. 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.
- The "Client Identification Practices Questionnaire" forms part of the identity proofing flow; completed questionnaires and the decisions of the Commission are recorded and retained (minutes SF 06.1.1.1).
- Where identification is performed by a partner acting as an external Registration Authority, each issuance is supported by the standardized request/declaration for issuing of a non-qualified certificate based on identification performed by an external Registration Authority (current version 1.1 / 04.11.2025), signed with a qualified electronic signature by an authorized representative of the partner; the declarations are validated upon receipt and retained as registration records (see M7). Evrotrust remains responsible for the conformity of registration performed by external Registration Authorities (ETSI EN 319 411-1, OVR-5.4.1-01).

M3 (Repository)

- Non-qualified certificates and their status information are published in a repository segment designated "non-qualified". All public references to the services hereunder avoid any wording or trust mark suggesting qualified status.

M4 (Profiles)

- Certificate, CRL and OCSP profiles for the non-qualified services are set out in the annex to this Practice Statement. They contain no QcStatements and carry the policy identifiers of eIDAS-CP-NQC-AES section 1.3, indicating the applied identity verification approach. The Annex distinguishes the Standard and Baseline LoIP policy identifiers for both natural-person AES certificates and legal-person AESeal certificates.

M5 (Subject keys)

- Subject keys are managed as per section 5 of eIDAS-CP-NQC-AES. Where Evrotrust provides a remote signature or seal creation component and manages the corresponding Subject keys, controls aligned with the applicable provisions of ETSI TS 119 431-1 are applied in accordance with the approved service configuration to support the Subject's sole control or, for legal persons, control over the private key. This reference does not assert use of a remote QSCD or full conformity of every service component with ETSI TS 119 431-1.

M6 (Audit)

- The non-qualified services are within the scope of the internal audit programme and the certified management systems of Evrotrust (ISO 9001, ISO/IEC 27001, ISO 20000-1, ISO 22301). They are not subject to mandatory conformity assessment under Article 20 of Regulation (EU) No 910/2014 or to mandatory prior notification; Evrotrust may inform the CRC voluntarily.

M7 (Records)

- Registration and identification records for non-qualified certificates, including completed questionnaires, attestations and assessment decisions, are retained for the same period and under the same protections as registration records under the Main CPS, that is for ten years after the certificate based on them ceases to be valid, under applicable Bulgarian legislation, satisfying the minimum retention required by ETSI EN 319 411-1 (OVR-6.4.6-01).

M8 (Legal)

- Liability follows Article 13 of Regulation (EU) No 910/2014 and Bulgarian law, including the Ordinance on the liability and termination of the activity of providers of certification services; Evrotrust maintains the insurance or resources required thereunder for the services hereunder.

- Article 19a of Regulation (EU) No 910/2014 and the applicable implementing acts for non-qualified trust services, including Commission Implementing Regulation (EU) 2025/2160, together with the applicable NIS2-related cybersecurity, incident-notification, supply-chain-security and accessibility requirements, are implemented through the common governance, risk-management, security and accessibility controls described in the Main CPS.

M9 (Terms and conditions)

- The terms and conditions for the non-qualified services comprise the General Terms and Conditions, the applicable certificate policy and the subscriber agreement. They include at minimum the elements of ETSI EN 319 411-1, OVR-6.9.4-02: certificate acceptance, the record retention period of ten years under applicable Bulgarian legislation, satisfying the minimum retention required by OVR-6.4.6-01, the obligations of subscribers and subjects (OVR-6.3.5-01, OVR-6.3.5-02), the notice to relying parties (OVR-6.3.5-03) and policy variances (OVR-7.2-01).
- A PKI disclosure statement following Annex A of ETSI EN 319 411-1 is published for each non-qualified certificate service.
- The GTC already regulate the existing non-qualified certificate for advanced electronic signature under item 2.2 and the non-qualified service for management of remote signature/seal creation devices, including short-term certificates for one-time signing (item 2.4.2). Certificates issued under the policies governed by this Practice Statement carry the applicable policy identifiers specified in section 1.3 of eIDAS-CP-NQC-AES.
- The contractual provisions applicable to any profile for one-time signing using an electronic seal shall be adopted before that profile is offered in production. This Practice Statement and eIDAS-CP-NQC-AES supplement, and do not replace, those provisions.

M10 (Limitations of use and liability)

- For the non-qualified services, the mechanism of the Main CPS section "Limitations of liability" (transaction value limits entered in qualified certificates) is adapted as follows: for the non-qualified services, any applicable reliance or transaction-value limit is indicated in the PKI Disclosure Statement (eIDAS-PDS-NQC-AES) and/or the Subscriber agreement or a service-specific notice. It is not represented in the certificate through QcStatements. The waiver-of-liability grounds of the Main CPS apply, supplemented by the approach-specific grounds in section 8.3 of eIDAS-CP-NQC-AES (reliance beyond the disclosed

identity verification approach; identity data declared or attested by the subscriber).

M11 (Signature process layer)

- Where Evrotrust provides the applicable signature or seal creation, augmentation or validation component, the processes based on non-qualified certificates follow ETSI EN 319 102-1 and the applicable format standards, as set out in the section "Signature creation and validation" of eIDAS-CP-NQC-AES. The related service configurations are maintained as internal controlled documents.

4 FUTURE NON-QUALIFIED SERVICES

A new non-qualified trust service is added to the scope of this Practice Statement by: (a) adoption of a service-specific policy (or policy annex) defining the service, its identifiers and any service-specific lifecycle rules; and (b) an annex hereto with the applicable profiles and any additional modifications. Sections 5, 6, 8 and 9 of the Main CPS as incorporated herein apply to any such service unchanged unless the annex states otherwise.

For services related to electronic attestations of attributes, Evrotrust will align the relevant annex with the applicable ETSI specifications for attribute attestation services once adopted as European standards.

5 ANNEX: CERTIFICATE, CRL AND OCSP PROFILES

5.1 PROFILE OF OPERATIONAL CERTIFYING AUTHORITY „EVROTRUST RSA ADVANCED OPERATIONAL CA 2025"

Version	V3	
Serial number	5a7dee700512557caa5abbbf10945f05192a35a5	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust Intermediate CA
	O=	Evrotrust Technologies JSC
	organization	NTRBG-203397356
	C=	BG
Valid from	02 April 2025 09:05:13 UTC	
Valid to	27 December 2030 09:05:12 UTC	
Subject	CN=	Evrotrust RSA Advanced Operational CA 2025
	O=	Evrotrust Technologies JSC
	organization Identifier (2.5.4.97)=	NTRBG-203397356
	C=	BG
Public Key Type/Length	RSA (3072 Bits)	
Subject Key Identifier	ccacd66b30366e791ea4a9545c7ff42ef04a3a29	
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	
Subject Alternative Name	RFC822 Name=evrotrustradvancedoperca2025@evrotrust.com URL=http://www.evrotrust.com	
Authority Key Identifier	KeyID=37138fdd6d141c71ff1b59fe56c732a289e5077b	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://services.evrotrust.com/EvrotrustIntermediateCA.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://services.evrotrust.com/EvrotrustIntermediateCA.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://services.evrotrust.com/ocsp
Key Usage (critical)	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=0

Thumbprint SHA256:
db13cd55c2ed043d3dfca91b62156c3359f81dfdccb3a8a512f78415e3ceb1e9

5.2 PROFILE OF OCSP RESPONDER „EVROTRUST RSA ADVANCED OPERATIONAL CA 2025 OCSP"

Version	V3	
Serial number	57eb68f7cb72ca857785e8b2db2175cb58f2e42d	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Advanced Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	Jul 25 08:04:46 2025 UTC	
Valid to	Jul 24 08:04:45 2030 UTC	
Subject	C= (countryName)	BG
	CN= (commonName)	Evrotrust RSA Advanced Operational CA 2025 OCSP
	OU= (organizationalUnitName)	OCSP Signing
	O = (organizationName)	Evrotrust Technologies JSC
	2.5.4.97 = (organizationIdentifier)	NTRBG-203397356
Public Key Type/Length	RSA 3072 Bits	
Subject Key Identifier	2110a567ac0a26dd26127b0d2d4c8a36e5a1a508	
Authority Key Identifier	Key ID=ccacd66b30366e791ea4a9545c7ff42ef04a3a29	
OCSP No Revocation	NULL (05 00)	

Checking	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAAdvancedOperationalCA2025.crl
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.4.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps
Basic Constraints (critical)	Subject Type=End Entity Path Length Constraint=None
Key Usage (critical)	Digital Signature, contentCommitment (formerly nonRepudiation) (c0)
Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)

Thumbprint SHA256:
050b08994160002a7109f1b5a45440d82e6329e6eb2bbde2826c661019fddfb1

5.3 PROFILE OF THE CRL OPERATIONAL CERTIFICATION AUTHORITY „EVROTRUST RSA ADVANCED OPERATIONAL CA 2025"

Version	V2	
Issuer	CN=	Evrotrust RSA Advanced Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Effective date	[effective date and time under UTC of validity of the issued CRL]	
Next update	[date and time under UTC of planned update of CRL]	
Signature Algorithm	SHA256RSA	
Signature hash algorithm	SHA256	
Authority Key Identifier	KeyID=ccacd66b30366e791ea4a9545c7ff42ef04a3a29	
CRL Number	[order number of CRL]	
expiredCertsOnCRL (OID=2.5.29.60)	[UTC date on which the CRL starts to keep revocation status information for expired certificates]	

5.4 PROFILE OF A NON-QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE OF A NATURAL PERSON "EVROTRUST ADVANCED NATURAL PERSON CERTIFICATE FOR AES – STANDARD"

Issued to natural persons by the certification authority "Evrotrust RSA Advanced Operational CA 2025" based on standard identity verification:

<table>
<tr><td>Version</td><td colspan="3">V3</td></tr>
<tr><td>Serial number</td><td colspan="3">[serial number]</td></tr>
<tr><td>Signature Algorithm</td><td colspan="3">SHA256RSA</td></tr>
<tr><td rowspan="4">Issuer</td><td colspan="2">CN=</td><td>Evrotrust RSA Advanced Operational CA 2025</td></tr>
<tr><td colspan="2">O=</td><td>Evrotrust Technologies JSC</td></tr>
<tr><td colspan="2">organizationIdentifier</td><td>NTRBG-203397356</td></tr>
<tr><td colspan="2">C=</td><td>BG</td></tr>
<tr><td>Valid from</td><td colspan="3">[starting date and time by UTC of the certificate validity]</td></tr>
<tr><td>Valid to</td><td colspan="3">[ending date and time by UTC of the certificate validity]</td></tr>
<tr><td rowspan="5">Subject[1]</td><td>C=
(countryName)</td><td colspan="2">Country: Two-letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.</td></tr>
<tr><td>CN=
(commonName)</td><td colspan="2">Common name: Selected by the natural person, with which he/she is normally introduced. When it is not selected, the full name of the natural person is entered.</td></tr>
<tr><td colspan="2"><table><tr><td>G=
(givenName)</td><td>Given name: Natural person name according to the identity document</td></tr><tr><td>S=
(surname)</td><td>Surname: Natural person surname according to the identity document</td></tr></table>Or<table><tr><td>2.5.4.65=
(pseudonym)</td><td>Pseudonym: Pseudonym, selected by the natural person</td></tr></table></td></tr>
<tr><td>SERIALNUMBER=
(serialNumber)</td><td colspan="2">Natural person identifier (ETSI EN 319 412-1 p.5.1.3), for example:
PNOBG-8310257645 for Civil Identification Number;
PASBG-12345678 for passport number;
IDCBG-195416023 for identity card number;</td></tr>
</table>

[1] Additional Subject DN attributes may be included, where required by the specific needs of a client and permitted by the applicable certificate profile.

		TINBG-123434341 for Tax Identification Number. If the person does not wish to enter his/her national identifier, a client number shall be entered, generated by the provider, to identify the individual if necessary.
	O = (organizationName) /optional/	Organization name: Full name of the organization under registration or act of entry by which the natural person is associated.
	2.5.4.97 = (organizationIdentifier) /optional/	Organization identifier (ETSI EN 319 412-1 p.5.1.4), for example: VARBG-123456789 – VAT; NTRBG-123456789 – UIC (BULSTAT). The national identifier according to the local law of the organization by which the natural person is associated is entered.
Public Key Type/Length	RSA (3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for the issued certificate]	
Authority Key Identifier	Key ID=ccacd66b30366e791ea4a9545c7ff42ef04a3a29	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAAdvancedOperationalCA2025.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/EvrotrustRSAAdvancedOperationalCA2025.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://services.evrotrust.com/ocsp	
Subject Alternative Name /optional/	RFC822 Name= [email address of the certificate Subject]	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.4.1.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps	

	[2]Certificate Policy: Policy Identifier=0.4.0.2042.1.3
Key Usage (critical)	contentCommitment (formerly nonRepudiation), Bit 1

5.5 PROFILE OF A NON-QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SIGNATURE OF A NATURAL PERSON "EVROTRUST ADVANCED NATURAL PERSON CERTIFICATE FOR AES – BASELINE LOIP"

Issued to natural persons by the certification authority "Evrotrust RSA Advanced Operational CA 2025" based on identity verification at Baseline LoIP:

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Advanced Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[starting date and time by UTC of the certificate validity]	
Valid to	[ending date and time by UTC of the certificate validity]	
Subject[2]	C= (countryName)	Country: Two-letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Common name: Selected by the natural person, with which he/she is normally introduced. When it is not selected, the full name of the natural person is entered.

[2] Additional Subject DN attributes may be included, where required by the specific needs of a client and permitted by the applicable certificate profile.

	G= (givenName)	Given name: Natural person name according to the identity document
	S= (surname)	Surname: Natural person surname according to the identity document
		Or
	2.5.4.65= (pseudonym)	Pseudonym: Pseudonym, selected by the natural person
	SERIALNUMBER= (serialNumber)	Natural person identifier (ETSI EN 319 412-1 p.5.1.3), for example: PNOBG-8310257645 for Civil Identification Number; PASBG-12345678 for passport number; IDCBG-195416023 for identity card number; TINBG-123434341 for Tax Identification Number. If the person does not wish to enter his/her national identifier, a client number shall be entered, generated by the provider, to identify the individual if necessary.
	O = (organizationName) /optional/	Organization name: Full name of the organization under registration or act of entry by which the natural person is associated.
	2.5.4.97 = (organizationIdentifier) /optional/	Organization identifier (ETSI EN 319 412-1 p.5.1.4), for example: VARBG-123456789 – VAT; NTRBG-123456789 – UIC (BULSTAT). The national identifier according to the local law of the organization by which the natural person is associated is entered.
Public Key Type/Length	RSA (3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for the issued certificate]	
Authority Key Identifier	Key ID=ccacd66b30366e791ea4a9545c7ff42ef04a3a29	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAAdvancedOperationalCA2025.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/EvrotrustRSAAdvancedOperationalCA2025.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://services.evrotrust.com/ocsp
Subject Alternative Name /optional/	RFC822 Name= [email address of the certificate Subject]
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.4.1.4.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.3
Key Usage (critical)	contentCommitment (formerly nonRepudiation), Bit 1

5.6 PROFILE OF A NON-QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SEAL OF A LEGAL PERSON "EVROTRUST ADVANCED LEGAL PERSON CERTIFICATE FOR AESEAL – STANDARD"

Issued to legal persons by the certification authority "Evrotrust RSA Advanced Operational CA 2025" based on standard identity verification:

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Advanced Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[starting date and time by UTC of the certificate validity]	
Valid to	[ending date and time by UTC of the certificate validity]	
Subject[3]	C= (countryName)	Country: Two-letter country code in conformity to ISO 3166. Specifies a general context in which other

[3] Additional Subject DN attributes may be included, where required by the specific needs of a client and permitted by the applicable certificate profile.

		attributes of Subject field are to be understood.
	CN= (commonName)	Legal entity/organisation name: Full name of the organization under registration or act of entry.
	O = (organizationName)	Legal entity/organisation name: Full name of the organization under registration or act of entry.
	2.5.4.97 = (organizationIdentifier)	Organization identifier (ETSI EN 319 412-1 p.5.1.4), for example: VARBG-123456789 – VAT; NTRBG-123456789 – UIC (BULSTAT). The national identifier according to the local law of the organization by which the legal person is entered.
Public Key Type/Length	RSA (3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for the issued certificate]	
Authority Key Identifier	Key ID=ccacd66b30366e791ea4a9545c7ff42ef04a3a29	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAAdvancedOperationalCA2025.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/EvrotrustRSAAdvancedOperationalCA2025.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://services.evrotrust.com/ocsp	
Subject Alternative Name /optional/	RFC822 Name= [email address of the certificate Subject]	
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.4.1.4.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.3	

Key Usage (critical)	contentCommitment (formerly nonRepudiation), Bit 1

5.7 PROFILE OF A NON-QUALIFIED CERTIFICATE FOR ADVANCED ELECTRONIC SEAL OF A LEGAL PERSON "EVROTRUST ADVANCED LEGAL PERSON CERTIFICATE FOR AESEAL – BASELINE LOIP"

Issued to legal persons by the certification authority "Evrotrust RSA Advanced Operational CA 2025" based on identity verification at Baseline LoIP:

Version	V3	
Serial number	[serial number]	
Signature Algorithm	SHA256RSA	
Issuer	CN=	Evrotrust RSA Advanced Operational CA 2025
	O=	Evrotrust Technologies JSC
	organizationIdentifier	NTRBG-203397356
	C=	BG
Valid from	[starting date and time by UTC of the certificate validity]	
Valid to	[ending date and time by UTC of the certificate validity]	
Subject[4]	C= (countryName)	Country: Two-letter country code in conformity to ISO 3166. Specifies a general context in which other attributes of Subject field are to be understood.
	CN= (commonName)	Legal entity/organisation name: Full name of the organization under registration or act of entry.
	O = (organizationName)	Legal entity/organisation name: Full name of the organization under registration or act of entry.
	2.5.4.97 = (organizationIdentifier)	Organization identifier (ETSI EN 319 412-1 p.5.1.4), for example: VARBG-123456789 – VAT; NTRBG-123456789 – UIC (BULSTAT). The national identifier according to the local law of the organization by which the legal person is entered.
Public Key Type/Length	RSA (3072/ 4096 Bits)	
Subject Key Identifier	[Calculated value for the issued certificate]	

[4] Additional Subject DN attributes may be included, where required by the specific needs of a client and permitted by the applicable certificate profile.

Authority Key Identifier	Key ID=ccacd66b30366e791ea4a9545c7ff42ef04a3a29
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://ca.evrotrust.com/crl/EvrotrustRSAAdvancedOperationalCA2025.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/EvrotrustRSAAdvancedOperationalCA2025.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://services.evrotrust.com/ocsp
Subject Alternative Name /optional/	RFC822 Name= [email address of the certificate Subject]
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.47272.4.1.4.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.evrotrust.com/cps [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.3
Key Usage (critical)	contentCommitment (formerly nonRepudiation), Bit 1

6 FINAL PROVISIONS

This Practice Statement is reviewed at least annually. It is published on the Evrotrust website. Questions and communications shall be addressed to the contacts indicated in the Main CPS.

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