Roksnet Certification Practice Statement

Document code: CPS
Version: 1.0
Published: 4 November 2026
Effective date: 5 November 2026
Publisher: Roksnet Solutions OÜ

This Certification Practice Statement describes how Roksnet Solutions OÜ implements the Roksnet Certificate Policy for SIGN and AUTH (version 1.0). It fills the technical implementation column of that policy. It is not a claim of conformance with ETSI EN 319 411-1 LCP and not a claim of qualified status.

1. Hierarchy

The hierarchy is:

- Roksnet Trust Service Root CA 2026, self-signed, pathLenConstraint 1, RSA-4096, sha384WithRSAEncryption, valid to 10 September 2036, no AIA. organizationIdentifier NTREE12998179.
- Roksnet Trust Service Intermediate CA 2026, pathLenConstraint 0, AIA http://ocsp.roksnet.com/CA, valid to 12 September 2031. Issues AUTH and SIGN certificates and its own OCSP responder certificates.
- Roksnet Trust Service TSA CA 2026, pathLenConstraint 0, AIA http://ocsp.roksnet.com/TSA, valid to 12 September 2031. Issues Timestamp Unit certificates and its own OCSP responder certificates.

There is no OCSP CA. The OCSP CA certificate was never issued. Each CA issues the OCSP responder certificate that answers for certificates it has issued, in accordance with RFC 6960.

From November 2026 the X-Road trust anchor is the Intermediate CA only. The Root is not yet a trust anchor. A Root-issued OCSP responder for CA-status is a later phase and requires reissue of the Intermediate and TSA CA certificates if their AIA is to point to http://ocsp.roksnet.com/ROOT.

2. Policy identifiers

CA certificates contain the policy identifier 1.3.6.1.4.1.47435.1.2. SIGN certificates contain 1.3.6.1.4.1.47435.1.2.1 and AUTH certificates 1.3.6.1.4.1.47435.1.2.2. The identifier of the Timestamp Policy is 1.3.6.1.4.1.47435.1.2.3. The CPS URI is https://www.roksnet.com/trustservices/cps. The LCP OID 0.4.0.2042.1.3 is not included.

3. Key management

The Root private key was generated and is held offline in an on-premises hardware module (YubiKey), under the Root Certificate Ceremonies Version 6.2. Intermediate CA and TSA CA private keys were generated inside Amazon AWS CloudHSM and remain inside that module, under the Intermediate CA Key and Certificate Generation Ceremony Version 1.2.

OCSP responder private keys are software keys managed by EJBCA Community Edition, because the free edition does not support AWS KMS. This remains until KMS support is available, after which new OCSP responder certificates will be issued with keys in KMS. Timestamp Unit private keys are held in AWS KMS. Subscriber private keys are generated on the Subscriber's X-Road Security Server. Roksnet does not hold Subscriber private keys and does not verify where they are stored. Hardware storage is recommended.

4. Certificate profiles

Profiles in force are the Root CA, Intermediate CA, TSA CA, OCSP responder, TSU, End-Entity Sign and End-Entity Auth profiles. End-entity organizationIdentifier uses the form

{scheme}{country}-{identifier} with schemes VAT, NTR, PSD, LEI, EOR and EXC, or a locally defined scheme of two characters followed by a colon. CA certificates retain NTREE12998179. SIGN key usage is nonRepudiation, critical. AUTH key usage is digitalSignature and keyEncipherment, critical, with clientAuth and serverAuth. AUTH keys are RSA of at least 2048 bits; SIGN keys are RSA of at least 2048 bits or ECDSA. No CRL Distribution Points extension is included.

5. Identification and issuance

The CA performs the registration function. The Subscriber is a Member identified in Roksnet Self-Service. With each application, submitted through the Member Account, the Subscriber provides the CSR, a signed statement and a document about the organisation. The CA checks the documents as set out in CA policy §§ 4–5, forms the certificate data from the result and verifies the CSR signature. The identity and authority of natural persons are not verified.

Two authorised Roksnet persons review the application and the CSR under dual control and approve the signature. The certificate is published to the Member Account for download, and the Subscriber confirms the certificate data before use. The issuance record links the application identifier, the Member Code, the Security Server, the CSR, the profile, the policy OID, the serial number, the designation stated by the Subscriber, if any, and the two approvers.

6. Revocation

A revocation request submitted through the Member Account that identifies the certificate is acted on no later than 24 hours after receipt. Reports of compromise that are not confirmed requests are investigated immediately and recorded. Revocation without the Subscriber's request is decided by Roksnet management. Revocation grounds are listed in the Trust Service Terms and Conditions. Status information is published only by OCSP. nextUpdate is thisUpdate plus 7 days. Archive cutoff is the issuing CA's validFrom date.

7. Certificate status service

OCSP for AUTH and SIGN is at http://ocsp.roksnet.com/CA. OCSP for Timestamp Unit certificates is at http://ocsp.roksnet.com/TSA. Responder certificates contain id-kp-OCSPSigning and id-pkix-ocsp-nocheck, and do not contain an Authority Information Access extension. The service is operated continuously; a single interruption lasts no more than 4 hours. Availability is monitored, and interruptions are logged with start, end and cause. The timestamping service is available continuously. A single interruption lasts no more than 4 hours. Its availability is monitored in the same way.

8. Publication

The CP, this CPS, the Timestamp Policy, the Terms, the profiles and the Root CA hash are published at https://www.roksnet.com/trustservices/cps and https://www.roksnet.com/resources. The Root hash publication address is https://www.roksnet.com/trustservices/rootca.

9. Records

The signed statements, the documents about the organisation and the records of acceptance, issuance, certificate confirmation and revocation are kept for ten years after the last related certificate ceases to be valid. Timestamping logs are kept as set out in the Timestamp Policy.

10. Personnel and physical controls

Trusted roles are Ceremony Administrator, Security Officer and System Administrator, with separation of duties. Dual control applies to CA key ceremonies and to end-entity certificate

signature. Root key material is held offline. Intermediate and TSA CA keys are held in CloudHSM. Access to EJBCA and to the CloudHSM is restricted to authorised personnel and is logged.

11. Cessation

If the service ceases, Roksnet will revoke outstanding certificates or arrange continued OCSP for their remaining validity, and will transfer or make available the records required to verify issued certificates and timestamps for the retention period. Subscribers are informed through their Member Account.