Roksnet Trust Service Terms and Conditions

Document code: TSTC

Version: 1.2

Published: 4 November 2026

Effective date: 5 November 2026

Publisher: Roksnet Solutions OÜ

These Terms apply to the issuance of authentication (AUTH) and signature (SIGN) certificates to organisations and to the provision of certificate status and timestamping services for data exchange through X-Road in the Roksnet Framework.

Provider	Roksnet Solutions OÜ
Registry code	12998179
Address	Keevise 10, 11415 Tallinn, Harjumaa, Estonia
Contact	support@roksnet.com
Services	AUTH certificates; SIGN certificates; OCSP; timestamping
Governing documents	These Terms; Roksnet CA Policies — SIGN and AUTH (the CA policy); the Certification Practice Statement (CPS); the Timestamp Policy; the certificate profiles; the Trust Services price list

1. Nature and scope

Roksnet Solutions OÜ ("Roksnet") is the certification authority and the timestamping authority for the services described here. The services are not qualified trust services under Regulation (EU) No 910/2014.

Certificates and timestamps are issued only for data exchange through X-Road in the Roksnet Framework. Seals and timestamps created in that exchange may be relied on as evidence of it.

SIGN and AUTH certificates are issued under Roksnet's own certificate policy, developed on the basis of ETSI EN 319 411-1 LCP. Conformance with LCP is not claimed, and the LCP OID is not included in certificates. SIGN certificates contain the policy identifier 1.3.6.1.4.1.47435.1.2.1 and AUTH certificates the policy identifier 1.3.6.1.4.1.47435.1.2.2. The CPS URI is https://www.roksnet.com/trustservices/cps.

These Terms form part of the Trust Services documentation. Capitalised terms have the meanings given in the Roksnet Terminology and Definitions (RTD) unless defined here. In case of conflict, these Terms prevail over the CA policy and the Timestamp Policy, and these prevail over the CPS and the certificate profiles. Fees are set only in the price list.

2. Subscriber

Subscriber has the meaning given in the RTD. Only a Member identified in Roksnet Self-Service can accept these Terms and use Trust Services, and it does so through its Member Account. Roksnet does not verify the identity or the authority of the natural person who uses the account.

3. Acceptance

Before its first certificate application, the Subscriber accepts these Terms by a separate explicit step in its Member Account. Roksnet records the version accepted, the date and time, and the account.

4. Certificate application

Certificate applications are submitted only through the Member Account. Each application includes the CSR generated on the Subscriber's Security Server, a statement signed by the Authorised Signatory and a document about the organisation: a document on its registration or incorporation or, for an organisation created by law, an official document or a confirmation from an official public list. Documents may be submitted in their original language. The content of the statement is set out in the CA policy (§ 4.2).

One application may cover AUTH and SIGN for one Security Server. AUTH is not a precondition for SIGN. Validity is 1, 2 or 3 years, as ordered.

The certificate data are taken from the data recorded in Self-Service and the documents submitted with the application. The organisation's name may be in its original language and script.

The Subscriber generates the key pair on its Security Server. Roksnet does not hold Subscriber private keys and does not verify where they are stored. Hardware storage is recommended. The Subscriber is responsible for the correctness of the data it submits and for the protection of the private key.

5. Delivery and confirmation

The issued certificate is made available in the Member Account. Before using it, the Subscriber confirms in the account that the certificate data are correct or reports an error. Downloading alone is not confirmation.

6. Certificate use and Subscriber obligations

AUTH certificates authenticate a Security Server. SIGN certificates are used to seal communication packages on the X-Road platform. Neither certificate is a qualified certificate.

The Subscriber shall:

- use a certificate only for its stated purpose in data exchange through X-Road in the Roksnet Framework;
- protect the private key;
- request revocation without delay if the key is compromised or the data in the certificate become incorrect;
- stop using a key for new operations once its compromise is detected;
- not use an expired or revoked certificate;
- not transfer a certificate or its private key to another legal person.

7. Revocation

A revocation request submitted through the Member Account that identifies the certificate is acted on no later than 24 hours after receipt. Other reports of possible compromise are registered and investigated; they are not by themselves a confirmed revocation request. If such a report cannot be confirmed within 24 hours, Roksnet records the action taken and the basis for it, as described in the CPS.

Roksnet revokes a certificate:

(a) on a revocation request from the Subscriber through its Member Account; (b) when the Member Account is closed; (c) when Roksnet establishes that the private key has been compromised or the certificate has been misused; (d) when Roksnet establishes that information in the certificate is inaccurate or that the certificate was not issued in accordance with the CA policy; (e) when Roksnet establishes that the organisation has ceased to exist; (f) when the Subscriber materially breaches these Terms; (g) when the private key of the issuing CA is compromised, or when Roksnet ceases to operate the CA without arrangements for another CA to continue status services.

Cancelling the Member Directory service does not affect issued certificates. When the Member Account is closed, Roksnet revokes all certificates issued to the Subscriber. Until then, the Subscriber requests revocation through its Member Account. Suspension of the Member Account does not prevent a revocation request through it.

8. Certificate status

The status of AUTH and SIGN certificates is available by OCSP at http://ocsp.roksnet.com/CA, continuously. A single interruption lasts no more than 4 hours. No certificate revocation list is published.

9. Timestamping

Timestamp tokens are produced by Timestamp Units certified by the TSA CA and are used only to timestamp messages and packages in X-Road data exchange. The service is not a qualified timestamping service. The timestamping service is available continuously. A single interruption lasts no more than 4 hours. Accuracy, time source and token format are stated in the Timestamp Policy.

10. Relying parties

A relying party verifies the certification path to the Roksnet CA it has decided to trust, the signature, the validity period and the key usage, and obtains a current OCSP response; it does not rely on a certificate reported as revoked or unknown. For a timestamp, it verifies the TSU signature, the status of the TSU certificate and that the hash matches the data relied on.

A certificate identifies the organisation. It does not confirm the identity of the person who operated the Member Account, the position of the Authorised Signatory or anyone's authority for a specific transaction.

A timestamp token shows that the timestamped data existed at the time stated in it. It does not prove the meaning of the data or who created them.

11. Fees

Fees and payment terms are set out in the Trust Services price list. Fees are exclusive of VAT.

12. Records and personal data

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 records are kept as set out in the Timestamp Policy.

Roksnet processes personal data in Trust Services as described in the Roksnet Privacy Notice for Services.

13. Complaints

Complaints about Trust Services are submitted through the Member Account or to support@roksnet.com. Roksnet registers each complaint and informs the Subscriber of the result.

14. Liability

Nothing in these Terms limits liability for wilful misconduct or any liability that cannot be limited under Estonian law.

Subject to the previous paragraph, Roksnet is not liable for:

- loss arising from the Subscriber's failure to protect a private key or to request revocation without delay;
- loss arising from reliance without the checks in section 10;
- loss arising from use of a certificate or timestamp outside the purpose stated in these Terms;
- indirect or consequential loss, or loss of profit, data or business;
- failure of networks, cloud infrastructure or the Subscriber's Security Server outside Roksnet's reasonable control.

Subject to the same reservation, Roksnet's total liability arising from a certificate is limited to the fee paid for that certificate, and its total liability arising from a timestamp is limited to the fees paid for the certificates of the requesting Security Server that were valid when the timestamp was produced.

15. Cessation of the CA

If Roksnet ceases the service, it will transfer or make available the records required for status information for the remaining validity of issued certificates, as described in the CPS.

16. Governing law and disputes

These Terms are governed by Estonian law. Disputes are subject to the exclusive jurisdiction of Harju County Court (Harju Maakohus), unless mandatory law provides otherwise.

17. Publication and changes

These Terms, the CA policy, the CPS, the Timestamp Policy, the certificate profiles and the Root CA hash are published at https://www.roksnet.com/trustservices/cps and https://www.roksnet.com/resources. Roksnet may amend these Terms with at least 30 days' prior notice for changes that are adverse to the Subscriber. The version in force at the time of an application applies to that application.