Timestamping Authority CA Certificate Profile

for Roksnet Trust Services

1. Document History

Document Version	Changes	Date
1	Initial version	15.03.2026
2	Introduction rewritten for TSA CA context; aligned algorithms, DN attributes, Certificate Policies, key identifiers and Key Usage; formatting aligned with Root CA, Intermediate CA and OCSP CA profiles; OCSP-only design (no CRL Distribution Points)	29.07.2026

2. Introduction

The Timestamping Authority CA (TSA CA) is a subordinate certification authority within the Roksnet Trust Services certification hierarchy. It is issued by the Roksnet Trust Service Root CA and is dedicated to issuing Timestamping Unit (TSU) certificates. These TSU certificates are used by the timestamping service to create and sign timestamps for communication packages exchanged on the X-Road-based data-exchange platform.

The TSA CA certificate is signed by the Roksnet Trust Service Root CA. The cryptographic hash of the Root CA certificate is published at https://www.roksnet.com/trustservices/rootca. The TSA CA certificate profile has been created in alignment with X.509 version 3, RFC 5280, RFC 3161 and Roksnet policy based on ETSI EN 319 411-1.

Because the Roksnet PKI is used exclusively within the X-Road data-exchange system, which relies solely on OCSP for certificate status information, the profile does not include CRL Distribution Points.

3. TSA CA Certificate Profile

Name of Field	Description	Value	Mandatory	Critical
CERTIFICATE BODY				
Version	Version of certificate data structure	V3	Y	NA
Serial number	Unique serial number for certificate identification		Y	NA
Signature algorithm	Algorithm used for signing certificate	sha384WithRSAEncryption or ecdsa-with-SHA384 (P-384)	Y	NA
Issuer	Distinguished name of the Root CA.CN: Root CA nameO: Organisation nameC: Country codeorganizationIdentifier : company registration number	CN = Roksnet Trust Service Root CA 2026 O = Roksnet Solutions OÜ C = EE organizationIdentifier = NTREE12998179	Y	NA
Valid from	Start date for certificate validity		Y	NA
Valid to	End date for certificate validity according to policy		Y	NA
Subject	The subject identifies the entity associated with the public key stored in the certificate.CN: TSA CA nameO: Organisation nameC: Country codeorganizationIdentifier : company registration number	CN = Roksnet Trust Service TSA CA 2026 O = Roksnet Solutions OÜ C = EE organizationIdentifier = NTREE12998179	Y	NA
Public key	Subject public key	RSA ≥ 4096 bits or ECC P-384 (or higher)	Y	NA

Signature value	Confirmation signature of the certificate issuer		Y	NA
CERTIFICATE EXTENSIONS				
Subject Key Identifier	Identifies the public key of the certificate holder	SHA-1 or SHA-256 hash of the public key	Y	N
Key Usage	Information about permitted use of certificate	keyCertSign, cRLSign	Y	Y
Basic Constraints	Indication of CA certificate	Subject Type = CAPath Length Constraint = 0	Y	Y
Certificate Policies	Policy OID	Policy Identifier: 1.3.6.1.4.1.47435.1.2 CPS URI: https://www.roksnet.com/trustservices/cps	Y	N
Authority Key Identifier	Identifies the public key used to sign the certificate / CRL	SHA-1 or SHA-256 hash of the issuer public key	Y	N
Authority Information Access	Authority information for certificate validation (OCSP only – X-Road requirement)	Access Method = id-ad-ocsp (1.3.6.1.5.5.7.48.1)URL = http://ocsp.roksnet.com/TSA	Y	N

Notes:

• Path Length Constraint = 0 ensures the TSA CA may only issue end-entity certificates (Timestamping Unit certificates) and may not issue further subordinate CAs.

• The Roksnet PKI is used exclusively for the X-Road data-exchange system, which requires OCSP and does not use CRLs. Consequently, CRL Distribution Points are not included in this profile.

• organizationIdentifier (OID 2.5.4.97) with the value NTREE12998179 is missing a dash between country code and numbers, as set in ETSI EN 319 412-1 clause 5.1.4. SerialNumber is retained for continuity.

• Private keys of the TSA CA shall be protected in a cryptographic module meeting the requirements of ETSI EN 319 411-1 clause 6.5.2 (e.g. AWS CloudHSM configured to FIPS 140-2 Level 3 or equivalent).

• Timestamping Unit (TSU) certificates issued under this CA shall contain the Extended Key Usage id-kp-timeStamping (1.3.6.1.5.5.7.3.8) marked critical, in accordance with RFC 3161.