Root CA Certificate Profile

for Roksnet Trust Services

1. Document History

Document Version	Changes	Date
1	Initial version	10.12.2025
2	Harmonised algorithms, DN attributes, Certificate Policies, CPS URI and public-key requirements.	29.07.2026

2. Introduction

The Root CA is the highest-ranking certification authority within the Roksnet Trust Services certification hierarchy. It is used to issue certificates for subordinate certification authorities (Intermediate CA and TSA CA).

The Root Certificate is a self-signed certificate. Its cryptographic hash is published at https://www.roksnet.com/trustservices/rootca. The Root certificate profile has been created in alignment with X.509 version 3, RFC 5280 and Roksnet policy based on ETSI EN 319 411-1.

The Path Length Constraint of 1 permits the Root CA to issue subordinate CA certificates that themselves may only issue end-entity certificates (pathLenConstraint = 0).

3. Root 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 certificate.CN: Root CA nameO: Organisation nameC: Country codeSerialNumber: company registration numberorganizationIdentifier: company registration number (ETSI)	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		Y	NA
Subject	The subject identifies the entity associated with the public key stored in the certificate.CN: Root CA nameO: Organisation nameC: Country codeSerialNumber: company registration numberorganizationIdentifier: company registration number (ETSI)	CN = Roksnet Trust Service Root 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 = CA Path Length Constraint = 1	Y	Y
Certificate Policies	Policy OID	Policy Identifier: 1.3.6.1.4.1.47435.1.2CPS URI: https://www.roksnet.com/trustservices/cps	Y	N
Authority Key Identifier	Identifies the public key used to sign the certificate / CRL (self-signed Root: typically identical to Subject Key Identifier or omitted)	SHA-1 or SHA-256 hash of the public key (optional for self-signed Root)	N	N

Notes:

• Path Length Constraint = 1 allows the Root CA to issue subordinate CA certificates (Intermediate CA, TSA CA). Each of those subordinate CAs must itself have pathLenConstraint = 0 so that they may issue only end-entity certificates.

• The Root certificate is self-signed; Issuer and Subject Distinguished Names are therefore identical. Authority Key Identifier may be omitted or set equal to the Subject Key Identifier.

• 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 key of the Root CA shall be protected in a cryptographic module meeting the requirements of ETSI EN 319 411-1 clause 6.5.2 (hardware security module, dual control, etc.).

• The cryptographic hash of the Root certificate shall be published at https://www.roksnet.com/trustservices/rootca (or the equivalent trust-services location).