End-Entity Auth Certificate Profile for Roksnet Trust Services

1. Document History

Document Version	Changes	Date
1	Initial version	08.01.2026
2	Policy OID per certificate type; Member Code; RSA keys only	13.10.2026
3	businessCategory removed; SIGN only	15.10.2026

2. Introduction

The Roksnet End-Entity certificates are issued by Roksnet intermediate CA to Roksnet members. Certificates are used within the Roksnet ecosystem to verify Security Server on X-Road platform.

End-Entity certificate profile is following X.509 version 3 and RFC 5280, and is aligned the Roksnet policy based on ETSI EN 319 411-1

3. End-Entity Certificate Profile

Name of Field	Description	Value	Man-datory	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	Y	NA
Issuer	Distinguished name of the intermediate CA certificate. CN: issuing CA name	CN = Roksnet Trust Service Intermediate CA 2026 O = Roksnet Solutions OÜ	Y	NA

	O: Organisation name C: Country code organizationIdentifier: company registration number	C = EE organizationIdentifier = NTREE12998179		
Valid from	Start date for certificate validity		Y	NA
Valid to	End date for certificate validity (validity time according to policy: 1, 2 or 3 years)		Y	NA
Subject	The subject identifies the entity associated with the public key stored in the certificate. CN: Member DNS/IP O: Organisation name C: Country code SerialNumber: Member Code organizationidentifier - according to ETSI EN 319 412-1 LEG-5.1.4-03	CN = *{Member DNS/IP}* O = *{Roksnet Member Legal name}* C = *{ISO 3166-1}* organizationIdentifier (2.5.4.97)= *{scheme}{country}-{identifier}* SerialNumber: {Member Code}	Y	NA
Public key	Subject public key	RSA ≥ 2048	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 hash of the public key	Y	N
Key Usage	information about permitted use of certificate	digitalSignature, keyEncipherment	Y	Y
Basic Constraints	Indication of CA certificate	Subject Type=End Entity Path Length Constraint=None	Y	N
Certificate Policies	Policy OID	Policy Identifier: 1.3.6.1.4.1.47435.1.2.2 CPS URI: https://www.roksnet.com/trustservices/cps	Y	N
Authority Key Identifier	Identifies public key of the issuer	SHA-1 hash of the public key	Y	N
Authority Information Access	Authority info: certificate validation information	Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) URL = http://ocsp.roksnet.com/CA	Y	N
Extended Key Usage		id-kp-clientAuth (1.3.6.1.5.5.7.3.2), id-kp-serverAuth (1.3.6.1.5.5.7.3.1)	Y	N