OCSP Certificate Profile for Roksnet Trust Services

1. Document History

Document Version	Changes	Date
1	Initial version	16.03.2026

2. Introduction

OCSP responder profile has been created in conformance with X.509 version 3, RFC 5280 and RFC 6960. Root CA and each intermediate level trust service (CA and/or TSA) issues OCSP responder certificates for corresponding OCSP service.

3. OCSP Responder Certificate Profile

Name of Field	Description	Value	Man-datory	Criti-cal
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	sha384RSA, sha384ECDSA	Y	NA
Issuer	Distinguished name of the issuing CA certificate. CN: CA name O: Organisation name C: Country code organizationIdentifier: issuer CA organizationIdentifier	CN = *[Roksnet Trust Service Root CA; or Roksnet Trust Service Intermediate CA; or Roksnet Trust Service TSA CA]* 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: OCSP name O: Organisation name C: Country code	CN = *[Roksnet Trust Service Root CA; or Roksnet Trust Service Intermediate CA; or Roksnet Trust Service TSA CA]* OCSP Responder v.*[4 -digit version number - YYMM]* O = Roksnet Solutions OÜ C = EE organizationIdentifier = NTREE12998179	Y	NA
Public key	Subject public key	RSA ≥ 4096, ECC 384	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
Authority Key Identifier	Identifies public key of issuer	SHA-1 hash of the public key	Y	N
Authority Information Access	Authority information for certificate validation (OCSP only – X-Road requirement) OCSP certificates has NoCheck		N	N
Key Usage	information about permitted use of certificate	DigitalSignature	Y	Y
Extended Key Usage	Additional purpose for Public Key usage	OCSP Signing (1.3.6.1.5.5.7.3.9) *[id-kp-OCSPSigning]*	Y	N
Basic Constraints	Indication of CA certificate	Subject Type End Entity	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
OCSP No Revocation Checking	RFC 6960, chapter 4.2.2.2.1	*OCSP NoCheck (1.3.6.1.5.5.7.48.1.5)* *[id-pkix-ocsp-nocheck]* = NULL	Y	N

4. OCSP Response Profile

Name of Field	Description	Value	Man-datory
ResponseStatus	Result of the query	0 for successful or error code	Y
ResponseBytes			Y
ResponseType	Type of the response	id-pkix-ocsp-basic	Y
BasicOCSPResponse			Y
tbsResponseData			Y
Version	Version of the response format	1	Y
responderID	Distinguished name of the OCSP responder. CN of the responder is named according to the underlying certificate	CN = *[Roksnet Trust Service Root CA; or Roksnet Trust Service Intermediate CA; or Roksnet Trust Service TSA CA]* OCSP Responder v.*[4 -digit version number - YYMM]* O = Roksnet Solutions OÜ C = EE organizationIdentifier = NTREE12998179	Y
producedAt	Date when the OCSP response was signed		Y
Responses			Y
certID	Serial number of the certificate		Y
certStatus	Status of the certificate: *GOOD* - certificate is issued and has not been revoked or suspended *REVOKED* - certificate is revoked or suspended *UNKNOWN* - the issuer of certificate is unrecognized by this OCSP responder, not issued by this CA		Y
revocationTime	Date of revocation or expiration of certificate		N
thisUpdate	Date when the status was queried from database		Y
Archive Cutoff	Archive cutoff date after a certificate has expired	CA's certificate "valid from" date.	Y
Extended Revoked Definition			N
nextUpdate	The time at or before which newer information will be	ThisUpdate + 7 days	Y

	available about the status of the certificate		
Nonce		Value is copied from request if it is included.	N
signatureAlgorithm		sha384RSAEncryption sha384ECDSAEncryption	Y
signature			Y
certificate		Certificate corresponding to the private key used to sign the response	Y