Timestamping Unit Certificate Profile for Roksnet Trust Services

1. Document History

Document Version	Changes	Date
1	Initial version	15.03.2026

2. Introduction

The Timestamp Unit (TSU) is issued by Roksnet Timestamping Authority Service CA (TSA). It is used to sign timestamps used in the X-Road platform.

TSU certificate profile has been created in conformance with X.509 version 3, RFC 5280, RFC 3161 and ETSI EN 319 422.

3. TSU 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	Signature algorithm used by the issuer (TSA CA)	sha384WithRSAEncryption	Y	NA
Issuer	Distinguished name of the certificate issuer. CN: TSA name O: Organisation name C: Country code	CN = Roksnet Trust Service TSA 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 policy		Y	NA
Subject	The subject identifies the entity associated with the public key stored in the certificate. CN: TSU name O: Organisation name C: Country code	CN = Roksnet Trust Service TSUx O = Roksnet Solutions OÜ C = EE organizationIdentifier = NTREE12998179	Y	NA
Public key	Subject public key type (TSU key)	RSA 4096, ECC 256, ECC 384	Y	NA
Signature value	Confirmation signature of the certificate issuer	sha384WithRSAEncryption	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	Y	Y
Extended Key Usage	Purpose for certificate public key usage	Time Stamping (1.3.6.1.5.5.7.3.8)	Y	Y
Certificate Policies	Policy OID	Policy Identifier: 1.3.6.1.4.1.47435.1.2.3 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/TSA	Y	N