

# **Qualified Time-Stamping Service**

## **Certificate Policy and Practice Statement**

QTSS-CPS

Unique object ID (OID): **1.3.6.1.4.1.57890.1.2.1**

Version 1.00

Valid since 2024-09-01

## Approvals

### Revision history

Version	Valid since	Description
1.00	2024-09-01	First official version of the document

### Approval of the document

	Name	Date	Signature
Reviewed by	Adomas Birštunas	2024-09-01	
Approved by	Antanas Mitašiūnas	2024-09-01	

## Table of content

<b>1. INTRODUCTION.....</b>	<b>5</b>
1.1. Overview .....	5
1.2. Identification .....	5
1.3. PKI participants .....	5
1.3.1. Certification authorities .....	6
1.3.2. Registration authorities .....	6
1.3.3. Subscribers .....	6
1.3.4. Relying parties .....	6
1.3.5. Other participants.....	6
1.4. Certificate usage .....	6
1.5. Policy administration .....	7
1.6. References.....	8
1.7. Definitions and abbreviations .....	9
<b>2. PUBLICATION AND REPOSITORY RESPONSIBILITIES .....</b>	<b>11</b>
<b>3. IDENTIFICATION AND AUTHENTICATION .....</b>	<b>12</b>
<b>4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS ..</b>	<b>13</b>
4.1. Certificate Application.....	13
4.2. Certificate application processing.....	13
4.3. Certificate issuance .....	13
4.4. Certificate acceptance.....	13
4.5. Key pair and certificate usage .....	13
4.6. Certificate renewal.....	13
4.7. Certificate re-key .....	13
4.7.1. Circumstance for certificate re-key.....	14
4.7.2. Who may request certification of a new public key .....	14
4.7.3. Processing certificate re-keying requests .....	14
4.7.4. Notification of new certificate issuance to subscriber.....	14
4.7.5. Conduct constituting acceptance of a re-keyed certificate .....	14
4.7.6. Publication of the re-keyed certificate by the CA .....	14
4.7.7. Notification of certificate issuance by the CA to other entities.....	14
4.8. Certificate modification .....	14
4.9. Certificate revocation and suspension.....	14
4.10. Certificate status services .....	15
4.11. End of subscription.....	15
4.12. Key escrow and recovery .....	15
<b>5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS...</b>	<b>16</b>
5.1. Physical controls .....	16
5.2. Procedural controls .....	16
5.3. Personnel controls.....	16

5.4. Audit logging procedures.....	16
5.5. Records archival .....	16
5.6. Key changeover .....	16
5.7. Compromise and disaster recovery.....	16
5.8. CA or RA termination .....	16
<b>6. TECHNICAL SECURITY CONTROLS .....</b>	<b>17</b>
6.1. Key pair generation and installation .....	17
6.2. Private Key Protection and Cryptographic Module Engineering Controls..	17
6.3. Other aspects of key pair management.....	17
6.4. Activation data.....	17
6.5. Computer security controls.....	17
6.6. Life cycle technical controls.....	17
<b>7. CERTIFICATE, CRL, AND OCSP PROFILES .....</b>	<b>18</b>
7.1. Certificate profiles.....	18
7.1.1. Root CA certificate profile .....	18
7.1.1.1 Certificate fields .....	18
7.1.1.2 Certificate extensions.....	19
7.1.2. TSU certificate profile.....	20
7.1.2.1 Certificate fields .....	20
7.1.2.2 Certificate extensions.....	21
7.2. CRL profiles .....	23
7.2.1. Profile of the CRL for TSU certificates .....	23
7.2.1.1 CRL fields .....	23
7.2.1.2 CRL extensions.....	23
7.3. OCSP profiles .....	24

## 1. INTRODUCTION

The joint stock company "MIT-SOFT" (further – the MitSoft) was established on August 1, 1991 and since 1996 is working in software development and services provision for creation and verification of electronic documents having the same legal effect as hand signed paper documents. Information about the MitSoft is available on the website <http://www.mitsoft.lt/>.

### 1.1. Overview

MitSoft Time-stamping Authority (TSA) is the authority issuing qualified electronic time stamps and also certificates used by MitSoft Qualified Time-Stamping Service (QTSS). MitSoft TSA Certificate Policy defines main requirements for certificates issued by MitSoft TSA. MitSoft TSA Certification Practice Statement defines practices used to implement requirements presented in MitSoft TSA Certificate Policy. MitSoft TSA Certificate Policy and MitSoft TSA Certificate Practice Statement are represented as one MitSoft TSA Certificate Policy and Practice Statement (CPS) document. Since MitSoft TSA issues certificates only for QTSS needs, this CPS document makes references to some parts of the [QTSS PS] document to avoid duplication of the requirements. CPS document is prepared considering requirements in the standard ETSI EN 319 411-1 [EN 319 411-1] and adopted them for QTSS needs.

Note regarding the definitions. Time stamps means qualified electronic time stamps as per Regulation (EU) 910/2014 [eIDAS]. Certificate Policy means MitSoft TSA Certificate Policy. Certification Practice Statement means MitSoft TSA Certification Practice Statement. MitSoft TSA or MitSoft QTSA means MitSoft Time-stamping Authority.

### 1.2. Identification

The unique identifier (OID) of the MitSoft TSA Certificate Policy is 1.3.6.1.4.1.57890.1.2.1; the values of its fields are given in the Table 1.

**Table 1.** The values of the fields of the unique identifier of the CP

Name	Value
ISO	1
Organization recognized by ISO	3
U.S. Department of Defence	6
Internet	1
Private company	4
Private company registered by IANA	1
Joint stock company "MIT-SOFT"	57890
Subdivision: Qualified trust services	1
Document type: MitSoft TSA Certificate Policy	2
Document version	1

### 1.3. PKI participants

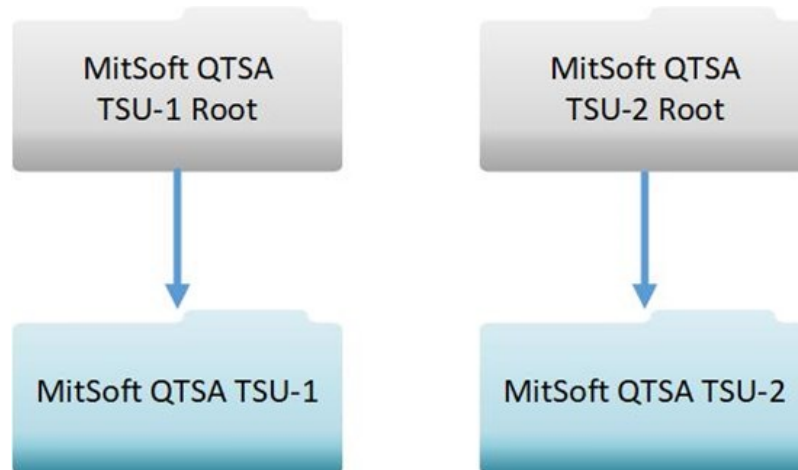
MitSoft TSA Certification authority is used as a certificate issuer for QTSS only. CA is not applicable for other applications. Therefore, there is no registration authority.

TSA issues certificates only for internal purposes of the MitSoft Qualified Time-stamping Service, and, therefore, it does not have its own subscribers.

### 1.3.1. Certification authorities

Two certificate hierarchies of identical structure are used. Keys and certificates of each certificate hierarchy reside in separate dedicated HSM. On the top of each hierarchy is a self-signed root CA certificate, which is used to issue TSU certificates and also for CRL signing.

Certificate hierarchies of TSA are presented in the following picture:



MitSoft TSA generates and stores keys of the self-signed root CA certificates and TSU certificates within the HSM, which is eIDAS certified as Qualified Signature Creation Devices and Qualified Seal Creation Device (QSCD). HSMs are secure cryptographic devices that provide EAL4+ level or higher in accordance with ISO/IEC 15408 [ISO 15408].

### 1.3.2. Registration authorities

Not applicable.

### 1.3.3. Subscribers

Not applicable.

### 1.3.4. Relying parties

TSA certificates are assumed to be used by the relying parties of MitSoft QTSS for qualified time stamp validation.

### 1.3.5. Other participants

Not applicable.

## 1.4. Certificate usage

Self-signed root CA certificates and their private keys are used only for issuance of TSU certificates for MitSoft Qualified Time-Stamping Service and for corresponding CRLs signing. Any other usage of the private keys of the self-signed root CA certificates is forbidden.

Issued TSU certificates and their private keys are used only by MitSoft Qualified Time-Stamping Service only for qualified electronic time stamps signing. Any other usage of the private keys of the TSU certificates is forbidden.

### **1.5. Policy administration**

MitSoft TSA Certificate Policy is managed by the joint stock company "MIT-SOFT", which contact information is given in the Table 2.

MitSoft TSA Certificate Policy and Practice Statement document is approved by the director of the joint stock company "MIT-SOFT".

**Table 2.** Contact information of the TSP

<b>TSA:</b>	The joint stock company "MIT-SOFT"
<b>Address:</b>	Kalvarijų str. 276-100, LT-08316 Vilnius
<b>Phone:</b>	+370 5 233 3922
<b>URL:</b>	<a href="https://www.mitsoft.lt/">https://www.mitsoft.lt/</a>
<b>E-mail:</b>	<a href="mailto:info@mitsoft.lt">info@mitsoft.lt</a>

## 1.6. References

- [eIDAS] - Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- [EN 319 401] - ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- [EN 319 411-1] - ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- [EN 319 412-1] - ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- [EN 319 412-3] - ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- [EN 319 421] - ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-stamps.
- [EN 319 422] - ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- [ISO 15408] - ISO/IEC 15408 (parts 1 to 3): Information security, cybersecurity and privacy protection -- Evaluation criteria for IT security.
- [ISO 27001] - ISO/IEC 27001:2022: "Information security, cybersecurity and privacy protection – Information security management systems - Requirements".
- [ISO 27002] - ISO/IEC 27002:2022: "Information security, cybersecurity and privacy protection – Information security controls".
- [ISO 27005] - ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection – Guidance on managing security risks".
- [RFC 5280] - RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
- [RFC 5480] - RFC 5480: Elliptic Curve Cryptography Subject Public Key Information.
- [TS 119 312] - ETSI TS 119 312 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" standard.
- [QTSS PS] - MitSoft "Qualified Time-Stamping Service Practice Statement", Version 1.00.

## 1.7. Definitions and abbreviations

**Certificate Policy:** named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

**Certification Practice Statement:** statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates.

**Compromise:** a loss, theft, modification, illegal use, or any other security violation of the confidential data.

**Coordinated Universal Time (UTC):** time scale based on the second as defined in Recommendation ITU-R TF.460-6 [1].

**Hardware security module (HSM), or cryptographic security module:** hardware and software used to generate cryptographic key pairs – private and public keys, to store private keys and/or to create electronic signatures.

**Relying party:** recipient of a time stamp who relies on that time stamp.

**Repository:** an internet place where information of the time-stamping service is made available for the users.

**Subscriber:** legal or natural person bound by agreement with a time-stamping trust service provider to any subscriber obligations.

**Time stamp:** data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time (= electronic time stamp [eIDAS]).

**Time-stamping:** electronic time stamp generation.

**Time-Stamping Authority (TSA):** TSP providing time-stamping services using one or more time-stamping units.

**Time-stamping service:** trust service for issuing time stamps.

**Time-Stamping Unit (TSU):** set of hardware and software which is managed as a unit and has a single time stamp signing key active at a time.

**Trust Service Provider (TSP):** entity which provides one or more trust services.

**Trusted list:** list that provides information about the status and the status history of the trust services from trust service providers regarding compliance with the applicable requirements and the relevant provisions of the applicable legislation.

**TSA practice statement/Time-stamping practice statement:** statement of the practices that a TSA employs in issuing time stamp.

NOTE: This is a specific type of trust service practice statement as defined in ETSI EN 319 401 [4].

<b>CA</b>	- Certification Authority
<b>CP</b>	- Certificate Policy
<b>CRL</b>	- Certificate Revocation List
<b>CPS</b>	- MitSoft TSA Certificate Policy and Practice Statement
<b>ESI</b>	- Electronic Signature and Infrastructure
<b>ETSI</b>	- European Telecommunications Standards Institute
<b>OID</b>	- Object identifier
<b>PS</b>	- Practice Statement
<b>QTSP</b>	- Qualified Trust Service Provider
<b>QTSS</b>	- Qualified Time-Stamping Service
<b>RRT</b>	- Communications Regulatory Authority of the Republic of Lithuania
<b>TSA</b>	- Time-Stamping authority

- TSP** - Trust Service Provider  
**TSU** - Time-Stamping Unit  
**UTC** - Coordinated Universal Time (fr. universel temps coordonné)

## **2. PUBLICATION AND REPOSITORY RESPONSIBILITIES**

All the certificates and CRLs are available in MitSoft repository. MitSoft repository is public and available for subscribers and relaying parties.

TSU certificates are published in the repository after their inclusion in the Trusted List of Lithuania.

The CRLs are also publicly available in MitSoft repository.

The frequency of publication of the regular CRL is at most 24 hours. Irregular CRL may be issued and published immediately after certificate revocation.

### **3. IDENTIFICATION AND AUTHENTICATION**

CA issues certificates only to MitSoft TSA itself and does not issue certificates to other subjects. Therefore, there are no requirements for identification and authentication of the identity and/or other attributes of an end-user certificate applicant to a CA.

Internal MitSoft TSA procedures are applied for key generation and TSU certificates for QTSS issuance. TSU certificate may be revoked only by the MitSoft TSA itself using internal procedures.

## **4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS**

Certificates are issued to MitSoft Qualified Time-stamping Service using internal procedures those implements requirements for TSU key generation defined in ETSI EN 319 421 [EN 319 421].

### **4.1. Certificate Application**

Not applicable.

### **4.2. Certificate application processing**

Not applicable.

### **4.3. Certificate issuance**

TSU certificates are issued to MitSoft Qualified Time-Stamping Service only. Other subscribers are not allowed to submit certificate applications.

Key generation for self-signed root CA certificates and TSU certificates, and the certificates issuance are performed only by trusted roles and under, at least, dual control ensured by internal procedures.

### **4.4. Certificate acceptance**

Not applicable.

### **4.5. Key pair and certificate usage**

The private keys of the root CA certificates may be used only for signing TSU certificates and corresponding CRLs. Any other usage of the private keys of the root CA certificates is forbidden.

The private keys of the TSU certificates may be used only for signing time-stamps issued by MitSoft Qualified Time-stamping Service. Any other usage of the private key of the TSU certificates is forbidden.

Private key shall not be used outside the private key usage period.

Relying parties should use TSU certificates and public keys for time-stamp validation and for TSU identification only.

### **4.6. Certificate renewal**

Certificate renewal (issuance of a new certificate without changing the public key) is not performed. Certificate re-key (issuance of a new certificate with a new public key) is used instead.

### **4.7. Certificate re-key**

Self-signed root CA certificates and TSU certificates re-key is performed by MitSoft TSA personnel using internal procedures satisfying the requirements for TSU key generation defined in ETSI EN 319 421 [EN 319 421]. MitSoft TSA ensures, that key pair generation and certificate issuance is performed by trusted roles only under, at least, dual control.

Cryptographic algorithms, key sizes and other fields of the certificates are described in the certificate profiles (see section 7.1. Certificate profiles).

#### **4.7.1. Circumstance for certificate re-key**

QTSS shall use valid TSU certificates with a non-expired private key usage period, therefore, MitSoft TSA ensures regular and timely TSU certificate re-key. In addition to regular TSU certificate re-key, TSU certificate re-key is performed if:

- data placed in the TSU certificate does not correspond to the legal status of TSA;
- cryptographic algorithms used for time stamp creation are changed, due to MitSoft QTSP business decision;
- TSU certificate profile was modified, due to its non-compliance with the requirements of the updated standards, legal acts or due to MitSoft TSA business decision;
- certificate revocation occurs.

Root CA certificate re-key is performed only because of its expiration or loss of the corresponding key.

#### **4.7.2. Who may request certification of a new public key**

Certificate re-key is performed by the MitSoft TSA request only.

#### **4.7.3. Processing certificate re-keying requests**

Not applicable.

#### **4.7.4. Notification of new certificate issuance to subscriber**

Not applicable.

#### **4.7.5. Conduct constituting acceptance of a re-keyed certificate**

Not applicable.

#### **4.7.6. Publication of the re-keyed certificate by the CA**

Newly issued certificates are published in the MitSoft repository.

#### **4.7.7. Notification of certificate issuance by the CA to other entities**

MitSoft TSA informs Communications Regulatory Authority of the Republic of Lithuania (RRT) performing role of National Supervisory Body of qualified trust service providers about new TSU certificate issuance for MitSoft QTSS. MitSoft TSA asks RRT to initiate the procedure for including a new TSU certificate in the Trusted list of Lithuania.

### **4.8. Certificate modification**

Certificate modification (issuance of a new certificate with updated attributes but without changing public key) is not performed. Certificate Re-key (issuance of a new certificate with a new public key) is used instead.

### **4.9. Certificate revocation and suspension**

TSU certificate revocation can be triggered by unexpected events such as loss of the TSU private key, or the official request from a law enforcement institution. In any

case, the investigation of the circumstances is performed and the revocation procedure is initiated only by the decision of the management of MitSoft.

Revocation is performed by the TSA personnel using internal procedures.

The information about revoked certificate is announced on the MitSoft website.

The subscribers of the MitSoft Qualified Time-Stamping Service are also informed via contact information provided to TSA by the subscribers.

Additionally, TSA informs Communications Regulatory Authority of the Republic of Lithuania (RRT) performing role of National Supervisory Body of qualified trust service providers about TSU certificate revocation. RRT may use its own procedures to inform other relying parties about TSU certificate revocation.

TSU certificate suspension is not applicable.

#### **4.10. Certificate status services**

MitSoft TSA provides CRLs as the certificate status service. The frequency of publication of the regular CRL is at most 24 hours.

CRLs are published in the MitSoft repository, and are publicly available for the MitSoft TSA subscribers and third parties.

Issued CRL fields are described in the CRL profile (section 7.2. CRL profiles).

Online Certificate Status Protocol (OCSP) is not supported.

#### **4.11. End of subscription**

Not applicable.

#### **4.12. Key escrow and recovery**

No backups of the private keys of the root CA certificates and TSU certificates are created. No recovery procedures are applied for the private keys of the root CA certificates and TSU certificates. On the loss of a private key:

- New key pair and new certificates are generated.
- While the new TSU certificate is issued and is included in the trusted list by the RRT, the other TSU will be used for time-stamping service.

## **5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**

MitSoft TSA uses the same physical and environmental security facilities, procedural and personal controls as for Qualified Time Stamping Service operation and management.

### **5.1. Physical controls**

Refer to clause 7.8 of [QTSS PS].

### **5.2. Procedural controls**

Refer to clause 7.3 of [QTSS PS].

### **5.3. Personnel controls**

Refer to clause 7.3 of [QTSS PS].

### **5.4. Audit logging procedures**

Refer to clause 7.12 of [QTSS PS].

Additionally:

- a) Records concerning all events relating to the life-cycle of the CA certificates and their keys are logged.
- b) Records concerning certificate revocation requests and reports of the performed actions are made.

### **5.5. Records archival**

Refer to clause 7.12 of [QTSS PS].

### **5.6. Key changeover**

Not Applicable.

### **5.7. Compromise and disaster recovery**

Refer to clauses 7.9 and 7.13 of [QTSS PS].

### **5.8. CA or RA termination**

Refer to clause 7.14 of [QTSS PS].

Additionally:

- a) private keys of the root CA certificates are destroyed in a manner such that the private keys cannot be retrieved.

## **6. TECHNICAL SECURITY CONTROLS**

### **6.1. Key pair generation and installation**

Key pair and certificate generation are performed only by trusted roles under, at least, dual control and are defined by the internal MitSoft TSA procedures.

Private keys are generated within a cryptographic module, and never exported from it, and never imported into it.

Key lengths and cryptographic algorithms for CA and TSU signing keys are selected according recommendations in ETSI TS 119 312 [TS 119 312].

Used cryptographic algorithms, key sizes, key usage purposes, validity periods and other fields and extensions of the created certificates are described in the certificate profiles (see section 7.1. Certificate profiles).

### **6.2. Private Key Protection and Cryptographic Module Engineering Controls**

Private signing keys are held and used within a cryptographic module, which assure EAL4+ level or higher in accordance with ISO/IEC 15408 [ISO 15408].

The same key protection requirements are applied for the private keys of the root CA certificates as for the private keys of the TSU certificates defined in the clause 7.6.3 of [QTSS PS].

### **6.3. Other aspects of key pair management**

Private key usage period is used for the keys of the TSU certificates. Details of the used private key usage period are defined in the certificate profile (see section 7.1. Certificate profiles).

### **6.4. Activation data**

Not Applicable.

### **6.5. Computer security controls**

Refer to clauses 7.5 of [QTSS PS].

### **6.6. Life cycle technical controls**

Refer to clauses 7.9 of [QTSS PS].

## 7. CERTIFICATE, CRL, AND OCSP PROFILES

### 7.1. Certificate profiles

#### 7.1.1. Root CA certificate profile

Self-signed root CA certificate is used only for issuing Certificates for MitSoft TSA. Root CA certificate profile defines X.509 version 3 certificate structure and it is conformant to RFC 5280 [RFC 5280] and ETSI EN 319 412-3 [EN 319 412-3].

##### 7.1.1.1 Certificate fields

Certificate fields for the certificate profile are presented in Table 1.

**Table 1.** Certificate fields for profile of the root CA certificate

Field	Required	Description	Possible values
Version	Yes	Describes the version of the encoded certificate	X.509 version 3 certificate (integer value is 2)
Serial Number	Yes	It is a positive integer assigned by the TSA to each certificate	<Randomly generated unique number of the certificate>
Issuer DN	Yes	Identifies the entity that has signed and issued the certificate	<Issuer distinguished name> <sup>1</sup> . DN contains the following attributes: <ul style="list-style-type: none"> <li>• C (countryName),</li> <li>• O (organizationName),</li> <li>• 2.5.4.97 (organizationIdentifier),</li> <li>• CN (commonName).</li> </ul> For example, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Subject DN	Yes	Identifies the entity associated with the public key stored in the subject public key field	<Subject distinguished name> <sup>1</sup> . DN contains the following attributes: <ul style="list-style-type: none"> <li>• C (countryName),</li> <li>• O (organizationName),</li> <li>• 2.5.4.97 (organizationIdentifier),</li> <li>• CN (commonName).</li> </ul> For example, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Not Before	Yes	Start of the certificate validity period. The certificate validity period is the time interval during which the TSA warrants that it will maintain information about the status of the certificate	<Date with time encoded with UTCTime>

<sup>1</sup> DN should be conformant to ETSI EN 319 412-3 [EN 319 412-3].

Not After	Yes	End of the certificate validity period. The certificate validity period is the time interval during which the TSA warrants that it will maintain information about the status of the certificate	<Date with time encoded with UTCTime>
Signature Algorithm	Yes	Contains the algorithm identifier for the algorithm used by the TSA to sign the certificate	ecdsa-with-SHA512 <sup>2</sup> (OID: 1.2.840.10045.4.3.4)
Subject Public Key	Yes	Is used to carry the public key and identify the algorithm with which the key is used	ECC public key <sup>2</sup> (OID: 1.2.840.10045.2.1) with P-521 elliptic curve <sup>3</sup> (OID: 1.3.132.0.35)
Signature Value	Yes	Contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate field	

### 7.1.1.2 Certificate extensions

Certificate extensions for the certificate profile are presented in Table 2.

**Table 2.** Certificate extensions for profile of the root CA certificate

Extension	Required	Critical	Description	Possible values
Subject Key Identifier (2.5.29.14)	Yes	No	Provides a means of identifying certificates that contain a particular public key	<SHA-1 hash of the subject public key>
Basic Constraints (2.5.29.19)	Yes	Yes	Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate	ca: TRUE; pathLenConstraint: 0
Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key contained in the certificate	keyCertSign (5), cRLSign (6)

<sup>2</sup> References to algorithm descriptions are presented in ETSI TS 119 312 [TS 119 312].

<sup>3</sup> Elliptic Curves are defined in RFC 5480 [RFC 5480].

## 7.1.2. TSU certificate profile

This profile defines inner structure of the certificate used by MitSoft TSA to sign qualified time stamps. TSU certificate is used only for signing qualified time stamps. TSU certificate profile defines X.509 version 3 certificate structure and it is conformant to RFC 5280 [RFC 5280] and ETSI EN 319 412-3 [EN 319 412-3].

The TSU certificate profile is aligned with requirements defined in ETSI EN 319 422 [EN 319 422].

### 7.1.2.1 Certificate fields

Certificate fields for the TSU certificate profile are presented in Table 3.

**Table 3.** Certificate fields for profile of the TSU certificate

Field	Required	Description	Possible values
Version	Yes	Describes the version of the encoded certificate	X.509 version 3 certificate (integer value is 2)
Serial Number	Yes	It is a positive integer assigned by the TSA to each certificate	<Randomly generated unique number of the certificate>
Issuer DN	Yes	Identifies the entity that has signed and issued the certificate	<Issuer distinguished name> <sup>4</sup> . DN contains the following attributes: <ul style="list-style-type: none"> <li>• C (countryName),</li> <li>• O (organizationName),</li> <li>• 2.5.4.97 (organizationIdentifier),</li> <li>• CN (commonName).</li> </ul> For example, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Subject DN	Yes	Identifies the entity associated with the public key stored in the subject public key field	<Subject distinguished name> <sup>4</sup> . DN contains the following attributes: <ul style="list-style-type: none"> <li>• C (countryName),</li> <li>• O (organizationName),</li> <li>• 2.5.4.97 (organizationIdentifier),</li> <li>• CN (commonName).</li> </ul> For example, "CN=MitSoft QTSA TSU-1, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
Not Before	Yes	Start of the certificate validity period. The certificate validity period is the time interval during which the TSA warrants that it will maintain information about the status of the certificate	<Date with time encoded with UTCTime>

<sup>4</sup> DN should be conformant to ETSI EN 319 412-3 [EN 319 412-3].

Not After	Yes	End of the certificate validity period. The certificate validity period is the time interval during which the TSA warrants that it will maintain information about the status of the certificate	<Date with time encoded with UTCTime>. Not After = Not Before + 2740 days
Signature Algorithm	Yes	Contains the algorithm identifier for the algorithm used by the TSA to sign the certificate	ecdsa-with-SHA512 <sup>5</sup> (OID: 1.2.840.10045.4.3.4)
Subject Public Key	Yes	Is used to carry the public key and identify the algorithm with which the key is used	ECC public key (OID: 1.2.840.10045.2.1) with P-384 elliptic curve <sup>6</sup> (OID: 1.3.132.0.34)
Signature Value	Yes	Contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate field	

**7.1.2.2 Certificate extensions**

Certificate extensions for the TSU certificate profile are presented in Table 4.

**Table 4.** Certificate extensions for profile of the TSU certificate

<b>Extension</b>	<b>Required</b>	<b>Critical</b>	<b>Description</b>	<b>Possible values</b>
Authority Key Identifier (2.5.29.35)	No	No	Provides a means of identifying the public key corresponding to the private key used to sign a certificate	<SHA-1 hash of the issuer public key>
Subject Key Identifier (2.5.29.14)	Yes	No	Provides a means of identifying certificates that contain a particular public key	<SHA-1 hash of the subject public key>
Basic Constraints (2.5.29.19)	No	Yes	Identifies whether the subject of the certificate is CA and the maximum depth of valid certification paths that include this certificate	cA: FALSE; pathLenConstraint: None
Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key contained in the certificate	digitalSignature (0)

<sup>5</sup> References to algorithm descriptions are presented in ETSI TS 119 312 [TS 119 312].

<sup>6</sup> Elliptic Curves are defined in RFC 5480 [RFC 5480].

Extended Key Usage (2.5.29.37)	Yes	Yes	Indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension	id-kp-timeStamping (1.3.6.1.5.5.7.3.8)
Certificate Policies (2.5.29.32)	Yes	No	Contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers	Certificate policyIdentifier: 1.3.6.1.4.1.57890.1.2.1, CPS qualifier (id-qt-cps): <URL that point to this CPS document>”
CRL Distribution Points (2.5.29.31)	Yes	No	Identifies how CRL information is obtained	DistributionPointName: <URL that points to a CRL that covers the certificate for all reasons>
Authority Information Access (1.3.6.1.5.5.7.1.1)	Yes	No	Indicates how to access information and services for the issuer of the certificate in which the extension appears	accessMethod: caIssuers (1.3.6.1.5.5.7.48.2), accessLocation: <URL that points to an issuer certificate>
Private Key Usage Period (2.5.29.16)	Yes	No	Used in order to limit the validity of the TSU's signing key	notBefore: <start time of the TSU's signing key usage>; notAfter: <end time of the TSU's signing key usage>. notAfter = notBefore + 3 years

## 7.2. CRL profiles

### 7.2.1. Profile of the CRL for TSU certificates

MitSoft Certificate Revocation Lists for TSU certificates are issued in accordance with RFC 5280 [RFC 5280].

#### 7.2.1.1 CRL fields

CRL fields for the CRL profile for TSU certificates are presented in Table 5.

**Table 5.** Fields for the CRL profile for TSU certificates

Field	Required	Description	Possible values
Version	Yes	Describes the version of the encoded CRL	version 2 CRL (integer value is 1)
Signature Algorithm	Yes	Contains the algorithm identifier for the algorithm used by the CRL issuer to sign the CertificateList	ecdsa-with-SHA512 <sup>7</sup> (OID: 1.2.840.10045.4.3.4)
Issuer Name	Yes	Identifies the entity that has signed and issued the CRL	<Issuer distinguished name> <sup>8</sup> . DN contains the following attributes: <ul style="list-style-type: none"> <li>• C (countryName),</li> <li>• O (organizationName),</li> <li>• 2.5.4.97 (organizationIdentifier),</li> <li>• CN (commonName).</li> </ul> For example, "CN=MitSoft QTSA TSU-1 Root, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
This Update	Yes	Indicates the issue date of this CRL	<Date with time encoded with UTCTime>
Next Update	Yes	Indicates the date by which the next CRL will be issued	<Date with time encoded with UTCTime>
Signature Value	Yes	Contains a digital signature computed upon the ASN.1 DER encoded tbsCertList field	
Revoked Certificates	No	Lists revoked certificates and their serial numbers if there exist revoked certificates	<List of revoked certificates> For every revoked certificate the following data should be presented: <ul style="list-style-type: none"> <li>• Certificate serial number,</li> <li>• Revocation date,</li> <li>• Revocation reason code according to RFC 5280</li> </ul>

#### 7.2.1.2 CRL extensions

Extensions for the CRL for TSU certificates profile are presented in Table 6.

<sup>7</sup> References to algorithm descriptions are presented in ETSI TS 119 312 [TS 119 312].

<sup>8</sup> DN should be conformant to ETSI EN 319 412-3 [EN 319 412-3].

**Table 6.** CRL extensions for the CRL profile for TSU certificates

<b>Extension</b>	<b>Required</b>	<b>Critical</b>	<b>Description</b>	<b>Possible values</b>
Authority Key Identifier (2.5.29.35)	Yes	No	Provides a means of identifying the public key corresponding to the private key used to sign a CRL	<Certificate subject key identifier of the CRL issuer>
CRL Number (2.5.29.20)	Yes	No	Contains a monotonically increasing sequence number for a given CRL scope and CRL issuer	<CRL sequence number>
Issuing Distribution Point (2.5.29.28)	Yes	Yes	Identifies the CRL distribution point and scope for a particular CRL, and it indicates whether the CRL covers revocation for end entity certificates only, TSA certificates only, attribute certificates only, or a limited set of reason codes	distributionPoint: <URL that points to a CRL that covers the certificate for all reasons>; onlyContainsUserCerts: False; onlyContainsCACerts: False; indirectCRL: False; onlyContainsAttributeCertificates: False; onlySomeReasons: not-used
ExpiredCertsOnCRL (2.5.29.60)	Yes	No	Indicates that a CRL containing this extension will include revocation status information for certificates that have been already expired	<NotBefore time of the CRL Issuer certificate>

**7.3. OCSP profiles**

Not Applicable.