mitsoft

Qualified Trust Service Provider

Certification Practice Statement

QTSP/CPS

Unique object ID (OID): **1.3.6.1.4.1.57890.2.1.1**

Version 1.00

Valid since 2026-07-01

UAB „MIT-SOFT“, Kalvarijų st. 276-100, LT-08316 Vilnius, Tel. +370 5 233 3922, www.mitsoft.lt, info@mitsoft.lt, Company ID 120792080, VAT payer code LT207920811

Approvals

Revision history

Version	Valid since	Description
1.00	2026-07-01	First official version of the document

Approval of the document

	Name	Date	Signature
Reviewed by	Adomas Birštunas	2026-06-18	
Approved by	Antanas Mitašiūnas	2026-06-19	

Table of content

1. INTRODUCTION 6
1.1. Overview 6
1.2. Identification 6
1.3. Application scope 7
1.4. Conformance 7
1.5. Contact information 7
2. References 8
3. Definitions and abbreviations 9
4. MitSoft QTSP CA: General Concepts 11
4.1. General policy requirements concepts 11
4.2. Certification Service applicable documentation 11
4.2.1. Certification Practice Statement 11
4.2.2. Certificate policies 11
4.2.3. Terms and conditions and PKI disclosure statement 12
4.3. Certification services 13
5. General provisions on Certification Practice Statement and Certificate Policies 15
5.1. General requirements 15
5.2. Certification Practice Statement 15
5.3. Certificate Policy name and identification 15
5.4. PKI participants 16
5.4.1. Certification Authority 16
5.4.1.1 MitSoft QTSP Root CA certificate 17
5.4.1.2 Certificates used by MitSoft QTSS 17
5.4.2. Subscriber and subject 18
5.4.3. Others 18
5.5. Certificate usage 18
6. Trust Service Providers practice 19
6.1. Publication and repository responsibilities 19
6.2. Identification and authentication 19
6.2.1. Naming 19
6.2.2. Initial identity validation 19
6.2.3. Identification and authentication for Re-key requests 19
6.2.4. Identification and authentication for revocation requests 19
6.3. Certificate Life-Cycle operational requirements 20
6.3.1. Certificate application 20
6.3.2. Certificate application processing 20
6.3.3. Certificate issuance 20

6.3.4. Certificate acceptance 20
6.3.5. Key pair and certificate usage 20
6.3.6. Certificate renewal 21
6.3.7. Certificate Re-key 21
6.3.8. Certificate modification 22
6.3.9. Certificate revocation and suspension 22
6.3.10. Certificate status services 22
6.3.11. End of subscription 22
6.3.12. Key escrow and recovery 22
6.4. Facility, management, and operational controls 23
6.4.1. General 23
6.4.2. Physical security controls 23
6.4.3. Procedural controls 23
6.4.4. Personnel controls 23
6.4.5. Audit logging procedures 24
6.4.6. Records archival 24
6.4.7. Key changeover 24
6.4.8. Compromise and disaster recovery 24
6.4.9. Certification Authority or Registration Authority termination 24
6.5. Technical security controls 25
6.5.1. Key pair generation and installation 25
6.5.2. Private key protection and cryptographic module engineering controls 25
6.5.3. Other aspects of key pair management 25
6.5.4. Activation data 26
6.5.5. Computer security controls 26
6.5.6. Life cycle security controls 26
6.5.7. Network security controls 26
6.5.8. Timestamping 26
6.6. Certificate, CRL and OCSP profiles 27
6.6.1. Certificate profiles 27
6.6.1.1 MitSoft QTSP Root CA certificate profile 27
6.6.1.1.1 Certificate fields 27
6.6.1.1.2 Certificate extensions 28
6.6.1.2 MitSoft QTSA CA certificate profile 29
6.6.1.2.1 Certificate fields 29
6.6.1.2.2 Certificate extensions 30
6.6.1.3 MitSoft QTSA TSU certificate profile 32
6.6.1.3.1 Certificate fields 32
6.6.1.3.2 Certificate extensions 33
6.6.2. CRL profiles 35

6.6.2.1 Profile of the CARL for MitSoft QTSA CA certificates 35
6.6.2.1.1 CARL fields 35
6.6.2.1.2 CARL extensions 36
6.6.2.2 Profile of the CRL for MitSoft QTSA TSU certificates 36
6.6.2.2.1 CRL fields 36
6.6.2.2.2 CRL extensions 37
6.6.3. OCSP profiles 38
6.7. Compliance audit and other assessment 39
6.8. Other business and legal matters 39
6.8.1. Fees 39
6.8.2. Financial responsibility 39
6.8.3. Confidentiality of business information 39
6.8.4. Privacy of personal information 39
6.8.5. Intellectual property rights 39
6.8.6. Representations and warranties 39
6.8.7. Disclaimers of warranties 39
6.8.8. Limitations of liability 39
6.8.9. Indemnities 39
6.8.10. Term and termination 39
6.8.11. Individual notices and communications with participants 40
6.8.12. Amendments 40
6.8.13. Dispute resolution procedures 40
6.8.14. Governing law 40
6.8.15. Compliance with applicable law 40
6.8.16. Miscellaneous provisions 40
6.9. Other provisions 40
6.9.1. Organizational 40
6.9.2. Additional testing 40
6.9.3. Disabilities 40
6.9.4. Terms and conditions 40

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/.

MitSoft is a qualified trust service provider (MitSoft QTSP), which offers different services including qualified trust services: qualified time-stamping service (QTSS) and qualified long-term preservation services (QLPS). MitSoft QTSP has internal certification authority, which issues certificates only for internal needs of the MitSoft QTSP trust services. This document is a certification practice statement (CPS) used by MitSoft QTSP CA for the certificate issuance for other MitSoft QTSP trust services.

1.1. Overview

MitSoft QTSP internal CA issues certificates to support trust services needs and according to certificate policy which is suitable for the particular trust service. Supported certificate policy may be a standard certificate policy as the one defined in standard ETSI EN 319 411-1 "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements", and/or some other certificate policy defined by the MitSoft QTSP CA itself. The same certification practice statement is used for all the certificate policies supported by MitSoft QTSP CA. The list of the certificate policies supported by this CPS is presented in the Table 3 (section 5.3).

The present CPS is based upon the following legal acts and normative documents:

a) The 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;

b) ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers";

c) ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements";

d) The Law on electronic identification and trust services for electronic transactions of the Republic of Lithuania issued on April 26, 2018.

Note regarding the definitions. Certification Practice Statement (or CPS) means MitSoft QTSP CA Certification Practice Statement. MitSoft QTSP means MitSoft Qualified Trust Service Provider.

1.2. Identification

The unique identifier (OID) of the MitSoft QTSP CA Certification Practice Statement is 1.3.6.1.4.1.57890.2.1.1; the values of its fields are given in the Table 1.

Table 1. The values of the fields of the unique identifier of the CPS

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: Non-qualified trust services	2
Document type: MitSoft QTSP CA Certification Practice Statement	1
Document version	1

The version of the CPS in effect is available on the website of MitSoft.

1.3. Application scope

MitSoft QTSP CA is an internal CA, which issues certificates only for the needs of the qualified trust services or trust services provided by MitSoft QTSP itself. MitSoft QTSP CA does not issue any certificates to external subjects and does not have any subscribers. MitSoft QTSP CA does not issue any certificates, those are not used to provide MitSoft QTSP trust services.

This peculiarity causes, that some common CA practices are not relevant, and not performed by MitSoft QTSP CA (for example, there is no registration service).

1.4. Conformance

MitSoft QTSP CA CPS document is prepared in accordance with the requirements of the standard ETSI EN 319 411-1 adopting them for MitSoft QTSP needs.

[NCP+] MitSoft QTSP confirms, that MitSoft QTSP CA is a trust service provider issuing certificates. MitSoft QTSP confirms, that certificate containing certificate policy extension with an OID value "0.4.0.2042.1.2", is issued in accordance with an extended Normalized Certificate Policy (NCP+) defined in the standard ETSI EN 319 411-1.

MitSoft QTSP CA Certification Practice Statement document is approved by the director of the joint stock company "MIT-SOFT".

1.5. Contact information

MitSoft QTSP CA CPS is managed by the joint stock company "MIT-SOFT", which contact information is given in the Table 2.

Table 2. Contact information of the QTSP

QTSP:	The joint stock company "MIT-SOFT"
Address:	Kalvarijų str. 276-100, LT-08316 Vilnius
Phone:	+370 5 233 3922
URL:	https://www.mitsoft.lt/
E-mail:	info@mitsoft.lt

2. 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.

[ENISA] - European Cybersecurity Certification Group, Sub-group on Cryptography: 'Agreed Cryptographic Mechanisms' published by the European Union Agency for Cybersecurity (ENISA).

[EN 319 401] – ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[EN 319 411-1] - ETSI EN 319 411-1: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

[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 319 422] – 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.

[QTS PS] - MitSoft "Qualified Trust Services Practice Statement".

[QTSS PS] - MitSoft "Qualified Time-Stamping Service Practice Statement".

[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.

3. 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.

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: natural or legal person that relies upon an electronic identification or a trust service.

Repository: an internet place where information of the services, provided by the trust service provider, is made available for the users.

Subscriber: legal or natural person bound by agreement with a trust service provider issuing certificates 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.

CA	–	Certification Authority
CARL	-	Certification Authority Revocation List
CP	-	Certificate Policy
CPS	-	MitSoft QTSP CA Certification Practice Statement
CRL	-	Certificate Revocation List
CSP	-	Certification Service Provider
ESI	–	Electronic Signature and Trust Infrastructure
ETSI	–	European Telecommunications Standards Institute
HSM	-	Hardware security module
OID	–	Object identifier
PS	-	Practice Statement
QTSP	–	Qualified Trust Service Provider
QTSS	–	Qualified Time-Stamping Service
RRT	–	Communications Regulatory Authority of the Republic of Lithuania

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

4. MitSoft QTSP CA: General Concepts

4.1. General policy requirements concepts

MitSoft QTSP CA provides certificates issuing service for other qualified trust services and trust services provided by MitSoft QTSP. The certificate issuing service is defined by the standard ETSI EN 319 411-1, while the common requirements are defined in the standard ETSI EN 319 401.

The section 4.2 provides the set of documents describing CA practices applied and how security is ensured.

MitSoft QTSP CA subdivisions involved into service provision and management described in the section 4.3.

4.2. Certification Service applicable documentation

Main documentation describing MitSoft QTSP CA certification service is the following:

- Certification practice statement;
- Certificate policies;
- Terms and conditions.

Terms and conditions are integrated in this Certification practice statement document.

4.2.1. Certification Practice Statement

Certification practice statement (this document) is a statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates. The CPS defines how the TSP meets the technical, organizational, and procedural requirements identified in the supported Certificate Policies.

ETSI EN 319 411-1 defines two types of the requirements for TSP issuing certificates: generic policy requirements common to all classes of trust service providers defined by ETSI EN 319 401 and certificate issuance-oriented requirements defined by ETSI EN 319 411-1 itself. Most of the generic requirements and their implementation are already defined by MitSoft in the MitSoft Qualified Trust Services Practice Statement [QTS PS] and, therefore, this document references [QTS PS] to avoid duplication. Specific certificate issuance-oriented requirements are defined in the present CPS document.

MitSoft QTSP internal CA issues certificates to support the needs of other trust services provided by MitSoft QTSP. This CPS document also references certification practice statements of the qualified trust services or trust services, those uses certificates issued by MitSoft QTSP CA.

4.2.2. Certificate policies

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

MitSoft QTSP CA may issue certificates for different trust services, provided by MitSoft QTSP, and may use different certificate policies depending on the service needs. The supported certificate policies may be the standard ones (defined in the standard ETSI EN 319 411-1) or some other certificate policies defined by the MitSoft QTSP itself. The same certification practice statement is used for all the certificate policies supported by MitSoft QTSP. The practices applicable only to particular certificate policy are distinguished in the CPS text by special marking.

The list of the certificate policies supported by the current version of the CPS of the MitSoft QTSP CA are the following:

- NCP+ (Normalized Certificate Policy requiring a secure cryptographic device) certificate policy defined in the standard ETSI EN 319 411-1. NCP+ certificate policy is used by MitSoft QTSP CA for issuing TSU and TSA certificates for MitSoft qualified time-stamping service (QTSS).

Note: current CPS supports the only one certificate policy, but the list of the supported certificate policies may be extended in the new CPS versions. Names and identification of the supported certificate policies are presented in a section 5.3.

There is no definition for the standard certificate policy, since it is already defined by the standard ETSI EN 319 411-1. Non-standard certificate policy would require a definition in the separate document or integration into CPS document.

ETSI EN 319 411-1 defines common requirements, those are applicable for any TSP issuing certificates, and also the list of specific requirements, those are applicable for particular standard certificate policies (NCP+ is one of the standard certificate policies). The practices defined in the present document include:

- practices applicable to any supported CP. Such practices are indicated by clauses without any additional marking;
- practices applicable only to the services offered under the NCP+ certificate policy. Such practices are indicated by clauses marked with "[NCP+]".

4.2.3. Terms and conditions and PKI disclosure statement

Terms and conditions of the certification service provided by MitSoft QTSP CA are the following:

1. Purpose. The MitSoft certification service provider (further - CSP) of the joint stock company "MIT-SOFT" (further – the MitSoft) discloses the general terms and conditions of the certification service to the relying parties and the subscribers of the MitSoft QTSP trust services. Certification service provided by the MitSoft CSP comply with the requirements stated in the 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, the Regulation (EU) No 2024/1183 of the European Parliament and of the Council of amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, and the standard ETSI EN 319 411-1 "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

2. Contact information. All issues concerning the certification service can be addressed to the contacts below:

Person: Antanas Mitašiūnas, the director of the joint stock company "MIT-SOFT"
Address: Kalvarijų st. 276-100, LT-08316 Vilnius
Phone: +370 5 233 3922
URL: https://www.mitsoft.lt/
E-mail: info@mitsoft.lt

3. Limitations on the use. CSP issues certificates only to trust services provided by MitSoft QTSP itself. Any external requests for certificate issuance are not allowed. CSP does not have any external subscribers or subjects. There are no direct contractual relationships between external subscribers and CSP. Only subscribers of other trust services provided by MitSoft QTSP may have interests indirectly related to this certification service. Third parties and subscribers of the MitSoft QTSP trust services may use certificates issued by CSP for trust service identification and validation only.

4. Certificate policies and certificate profiles. CSP issues certificates under the certificate policies declared in issued certificates and conforms certificate profiles defined in this Practice Statement:

- Certificates issued for MitSoft Qualified Time-Stamping Service are issued under the NCP+ (Normalized Certificate Policy requiring a secure cryptographic device) certificate policy (an OID value "0.4.0.2042.1.2") defined in ETSI EN 319 411-1.

5. Relying party obligations. The relying party obligations are to accept this certification service terms and conditions and take any other measures of precaution. The relying party, when relying upon a certificate, shall verify certificate validity and its revocation status.

6. Verification of a certificate validity. Certificate validation should be performed in accordance with standards and taking into the account certificate proof-of-existence, certificate validity period, revocation status and hash, and signature algorithms reliability. For revocation checking CRL should be used.

7. Event logs. The journals of CSP system operation and activity registration (event logs), which can be used as legal evidence, when necessary, are maintained for two years.

8. Applicable law. CSP operates in the Republic of Lithuania and follows EU and Lithuanian laws and normative legal acts. The main laws and normative legal acts are the following:

- The 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;
- ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers";
- ETSI EN 319 411-1: "Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements";
- The Law on electronic identification and trust services for electronic transactions of the Republic of Lithuania issued on April 26, 2018.

9. Settlement of disputes and complaints. All the complaints and disputes between CSP and its users are resolved by positive-minded negotiations. In a case of failing to settle a dispute, it is addressed to the institutions of law enforcement.

10. Liability, warranty and its limitations. CSP is liable for its illegal operation and reimburses the harm incurred by the subscriber of the trust services compelled by the law of the Republic of Lithuania. CSP undertakes no additional obligations, except for those determined in the subscriber agreements for provision of trust service, certificates are issued to.

11. Applicable agreements and practice statement. CSP provides certificates according to the certificate policies declared in the corresponding certificates, following the Practice statement (OID: 1.3.6.1.4.1.57890.2.1.1), this Terms and Conditions as well as the subscriber agreements of the trust services, certificates are issued to.

12. Privacy policy. CSP ensures that the requirements of the European Data Protection Directive 95/46/EC, as it is implemented through Lithuanian legislation, are met.

4.3. Certification services

The certification services are broken down by the ETSI EN 319 411-1 into the following component services:

- Registration service: verifies the identity and if applicable, any specific attributes of a subject.

- Certificate generation service: creates and signs certificates based on the identity and other attributes verified by the registration service. This can include key generation.
- Dissemination service: disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the TSP's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- Revocation management service: processes requests and reports relating to revocation to determine the necessary action to be taken.
- Revocation status service: provides certificate revocation status information to relying parties.
- Subject device provision service: prepares, and provides or makes available secure cryptographic devices, or other secure devices, to subjects.

MitSoft QTSP CA is an internal CA, which issues certificates only to support other qualified trust services or trust services provided by MitSoft QTSP. MitSoft QTSP CA does not issue certificates for external subjects, does not need to identify, verify or store attributes of the subjects, does not need to provide keys to subjects, and does not need to accept revocations requests from the external parties.

All the mentioned above leads to MitSoft QTSP CA does not have some of the component services defined by the standard ETSI EN 319 411-1, or some of these component services are restricted:

- Registration service: MitSoft QTSP CA does not have registration service, since there are no external subjects.
- Certificate generation service: generates keys, creates and signs certificates issued to MitSoft QTSP trust service.
- Dissemination service: it is restricted to publishing practice statements, terms and conditions, and certificates to relying parties only.
- Revocation management service: it is limited to describing practice of certificate revocation by the request of MitSoft QTSP itself.
- Revocation status service: provides certificate revocation status information to relying parties.
- Subject device provision service: MitSoft QTSP CA does not have subject device provision service, since there are no external subjects.

5. General provisions on Certification Practice Statement and Certificate Policies

5.1. General requirements

Certificates issued by MitSoft QTSP CA are issued according requirements listed in ETSI EN 319 411-1. The implementation of the requirements is based on the practices presented in this CPS document and other supplementary document.

5.2. Certification Practice Statement

Refer to clause 6.1 of [QTS PS].

Additionally, for providing certificate issuance service:

a) The practices and procedures used to address the requirements identified in certificate policies supported by MitSoft QTSP CA are described in the present Certification Practice Statement.

b) The MitSoft QTSP CA identifies the obligations of all external organizations supporting the QTSP CA services including the applicable policies and practices.

c) CPS defines certificate profiles, including used signature algorithms, certificate fields, and certificate extensions for every certificate issued according to certificate policies supported by MitSoft QTSP CA.

d) CPS and other relevant documentation are publicly available to relying parties on the MitSoft repository on a 24X7 bases.

Disclosure statement of MitSoft QTSP CA is specified in Terms and Conditions of the certification service (see section 4.2.3).

5.3. Certificate Policy name and identification

MitSoft QTSP CA may issue certificates according different certificate policies to meet the needs of other trusted services provided by MitSoft QTSP. The same CPS is used for all the certificate policies supported by MitSoft QTSP CA.

The list of the supported certificate policies, their names and identification are listed in the Table 3.

Table 3. Certificate policies supported by CPS.

CP name	CP identifier (OID)	CP describing document	Trust service, which uses CP
NCP+: "Normalized Certificate Policy requiring a secure cryptographic device"	0.4.0.2042.1.2	ETSI EN 319 411-1	MitSoft qualified time-stamping service (QTSS) for issuing TSU and TSA certificates

Note: current CPS supports the only one certificate policy, but the list of the supported certificate policies may be extended in the new CPS versions.

5.4. PKI participants

MitSoft QTSP Certification authority is used as a certificate issuer only for qualified trust services and trust services provided by MitSoft QTSP itself. CA is not suitable for other applications.

5.4.1. Certification Authority

MitSoft QTSP CA uses 3-level certificate hierarchy:

- MitSoft QTSP Root CA certificate is a self-signed certificate presented on the top of the hierarchy. MitSoft QTSP Root CA certificate is used only to issue MitSoft QTSP service root certificates.
- MitSoft QTSP service root certificates are CA certificates issued by MitSoft QTSP Root CA and presented in the middle of the hierarchy. Each MitSoft QTSP service root certificate is dedicated to particular trust service provided by MitSoft QTSP. There may be zero, one or several service root certificates issued for the single trust service. MitSoft QTSP service root certificate is used only to issue service certificates.
- MitSoft QTSP service certificates are an end-entity certificates directly used for the provision of the particular trust service.

Current certificate hierarchy of MitSoft QTSP CA is presented in the Fig. 1.

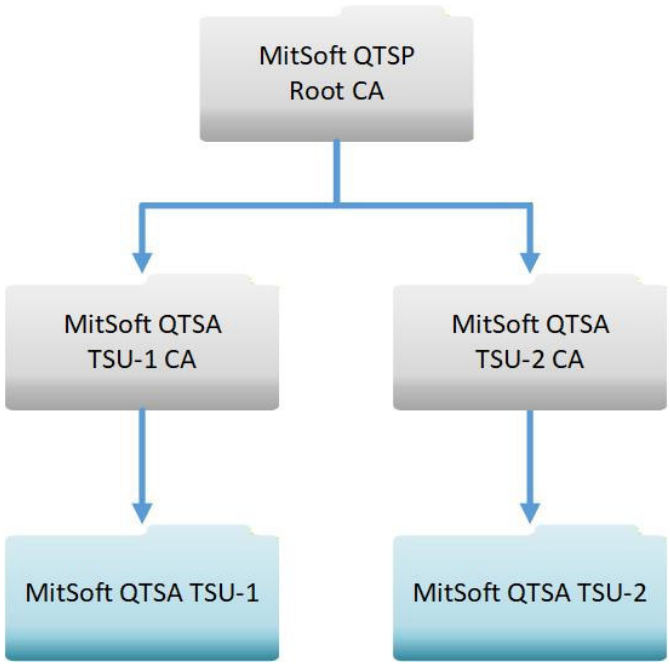


Fig 1. Certificate hierarchy of MitSoft QTSP CA

Here:

- MitSoft QTSA TSU-1 CA and MitSoft QTSA TSU-2 CA certificates are MitSoft QTSP service root certificates dedicated to MitSoft qualified time-stamping service (QTSS) and used to issue service certificates.
- MitSoft QTSA TSU-1 and MitSoft QTSA TSU-2 certificates are MitSoft QTSP service certificates dedicated to MitSoft qualified time-stamping service (QTSS) and used directly for time stamp provision.

5.4.1.1 MitSoft QTSP Root CA certificate

MitSoft QTSP Root CA is a self-signed certificate, those key pair is generated and stored within separate dedicated cryptographic security module (HSM). Cryptographic security module containing keys of the MitSoft QTSP Root CA is stored in a high security zone - specific physical location of the security zone, which is physically isolated from normal operations. Only personnel in trusted roles have access to high security zone and to cryptographic security module. Cryptographic security module containing keys of the MitSoft QTSP Root CA is kept disconnected from network. Director of the MitSoft has overall responsibility for secure storage of the cryptographic security module, which keeps private key of the MitSoft QTSP Root CA certificate.

Key pair of the MitSoft QTSP Root CA are generated according MitSoft QTSP Root CA key generation ceremony, which ensures the following:

- key pair is generated within dedicated HSM and conforms key pair generation procedures defined by the HSM manufacture;
- the integrity and confidentiality of the key pair is ensured; private key is not extracted from the HSM and not imported into the HSM;
- ceremony is performed by trusted roles only;
- ceremony is performed under, at least, dual control;
- ceremony is observed by security officer and independent observer;
- ceremony is performed using secure software and hardware suitable for this purpose;
- algorithms and key lengths are compliant with the requirements of ETSI EN 119 312 and ENISA;
- generated MitSoft QTSP Root CA certificate is compliant with a certificate profile for MitSoft QTSP Root CA certificate defined in this CPS (see section 6.6.1.1);
- HSM was placed and stored in a high security zone and physically isolated from normal operations;
- appropriate evidences of the ceremony were collected and stored;
- the ceremony report was created and signed by the security officer and independent trustworthy person - ceremony observer.

No backups of the private key of the MitSoft QTSP Root CA are created. On the loss of a private key (or access to it), new key pair and new certificate is generated.

5.4.1.2 Certificates used by MitSoft QTSS

MitSoft QTSP provides qualified time-stamping service (QTSS) using 2 time-stamping units – TSU1 and TSU2. Two certificate sub-hierarchies for every TSU of identical structure are used. Keys and certificates of each TSU certificate sub-hierarchy reside in a separate dedicated HSM.

QTSS uses certificates issued by MitSoft QTSP internal CA. Service root certificates for QTSS are issued by MitSoft QTSP Root CA and used as CA certificates for issuing TSU certificates only.

Service root certificates for QTSS are:

- MitSoft QTSA TSU1 CA certificate, to be used for issuing TSU certificate for TSU1 and also for corresponding CRL signing;
- MitSoft QTSA TSU2 CA certificate, to be used for issuing TSU certificate for TSU2 and also for corresponding CRL signing.

TSU certificates are service certificates used by QTSS for signing time stamps only.

TSU certificate used by TSU1 are issued by MitSoft QTSA TSU1 CA certificate, and keys, associated with TSU1 certificates and MitSoft QTSA TSU1 CA certificate, are generated and stored in HSM dedicated to TSU1.

TSU certificate used by TSU2 are issued by MitSoft QTSA TSU2 CA certificate, and keys, associated with TSU2 certificates and MitSoft QTSA TSU2 CA certificate, are generated and stored in HSM dedicated to TSU2.

[NCP+] Service root certificates for QTSS are issued under NCP+ certificate policy in accordance with a certificate profile presented in the section 6.6.1.2.

[NCP+] TSU certificates are issued under NCP+ certificate policy in accordance with a certificate profile presented in the section 6.6.1.3.

[NCP+] MitSoft QTSP CA generates and stores keys of the service root certificates for QTSS and TSU certificates within the HSMs, which are 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.

5.4.2. Subscriber and subject

MitSoft QTSP CA does not issue certificates to subjects other than MitSoft QTSP itself. MitSoft QTPS CA does not have any subscribers or customers bounded by contracts.

5.4.3. Others

No other participants, except MitSoft QTSP itself, are identified by this CPS.

5.5. Certificate usage

Certificates issued by MitSoft QTSP internal CA are used only by trust services provided by MitSoft QTSP itself.

Self-signed MitSoft QTSP Root CA certificate and its private key is used only for issuance of MitSoft QTSP service root certificates and CARL signing. Any other usage of the private key of the MitSoft QTSP Root CA certificate is forbidden.

MitSoft QTSP service root certificates are used only as CA certificates for service certificate issuance and CRL signing. Any other usage of the private keys of the MitSoft QTSP service root certificates are forbidden.

MitSoft QTSP service certificates are end-entity certificates directly used in a particular trust service provision. The usage depends on the trust service provided and is more precisely defined in a corresponding trust service documentation.

6. Trust Service Providers practice

6.1. Publication and repository responsibilities

All the certificates issued by MitSoft QTSP Root CA (including itself and certificates issued by subordinate CAs) and CRLs are available in MitSoft repository. MitSoft repository is public and internationally available for subscribers and relying parties 24 hours per day, 7 days per week.

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.

Certification practice statement document is available for the relying parties in the MitSoft repository. Terms and conditions are available to the relying parties as part of this CPS document (see section 4.2.3).

6.2. Identification and authentication

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

6.2.1. Naming

Naming used in the certificate profiles is aligned with the requirements in the RFC 5280 and ETSI EN 319 412-3.

6.2.2. Initial identity validation

MitSoft QTSP CA does not issue certificates for external subscribers or subjects. Therefore, identity and attribute validation are non-applicable.

MitSoft QTSP CA CPS, certificate profiles, and practice statements of the trust services (provided by MitSoft QTSP) define attributes used in the trust service certificates issued to MitSoft QTSP.

6.2.3. Identification and authentication for Re-key requests

Non-applicable. MitSoft QTSP CA does not accept any Re-key requests.

6.2.4. Identification and authentication for revocation requests

MitSoft QTSP CA does not accept any external revocation requests.

CA and end-entity certificates issued by MitSoft QTSP CA may be revoked only by the request of MitSoft QTSP itself using internal procedures. In the case of revocation, status is published through the CRL or CARL. Depending on the trust service, that certificate was revoked, additional notification to the relying parties may be provided if it is defined in the corresponding trust service practices.

CRLs and CARLs are published in a publicly available MitSoft repository. Times used for CRL generation are synchronized with UTC at least once every 24 hours.

6.3. Certificate Life-Cycle operational requirements

6.3.1. Certificate application

Non-applicable. MitSoft QTSP CA does not accept any certificate applications from external subscribers.

6.3.2. Certificate application processing

Non-applicable.

6.3.3. Certificate issuance

Service root certificates and service certificates are issued to MitSoft QTSP trust services only. Internal procedures are used for certificate issuance.

Key generation for service root CA certificates and for service certificates, and the certificates issuance are performed only by trusted roles.

[NCP+] If service root CA certificates or service certificates are issued under NCP+ certificate policy, key generation and the certificates issuance are performed in a secure environment and only under, at least, dual control ensured by internal procedures.

Service root CA certificates and service certificates are issued in accordance with corresponding certificate profiles, which define in detail the values of the certificate fields and certificate extensions used.

[NCP+] If service root CA certificates or service certificates are issued under NCP+ certificate policy, key and certificate generation are performed within HSM using HSM middleware, which ensures security and randomness for certificate serial.

Algorithms and key lengths used for key generation are presented in the certificate profiles (see section 6.6.1) and are compliant with the requirements of ETSI EN 119 312 and ENISA.

Issued certificates are published in the MitSoft repository.

In the case service certificate is used for qualified trust service identification, MitSoft QTSP informs Communications Regulatory Authority of the Republic of Lithuania (RRT) performing role of National Supervisory Body of qualified trust service providers about new certificate issuance for the corresponding qualified trust service provided by MitSoft QTSP. MitSoft QTSP asks RRT to initiate the procedure for including a new service certificate in the Trusted list of Lithuania. Particular trust service practice statement may define additional notifications for relying parties about issuance of the new certificate.

6.3.4. Certificate acceptance

Non-applicable.

6.3.5. Key pair and certificate usage

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

[NCP+] If service root CA certificates are issued under NCP+ certificate policy, private keys of the service root CA certificates are used only within secure cryptographic device (HSM).

Obligations for the MitSoft trust services for which a service certificate has been issued:

a) the private keys of the service certificates may be used only for purposes defined in section 5.4.1 and in accordance practices defined by the MitSoft QTSP trust service;

b) MitSoft trust service shall ensure protection against unauthorized private key use;
c) [NCP+] If service certificate is issued under NCP+ certificate policy, private key is used only within secure cryptographic device (HSM);
d) in the case control over private key is lost, inform MitSoft QTSP internal CA and take actions to stop using private key for service providing;
e) in the case service certificate is revoked by MitSoft QTSP, take actions to stop using private key for service providing.

Private keys are not used outside the private key usage period.

Relying parties should use MitSoft QTSP service certificates and public keys only for purposes described by the MitSoft QTSP trust service (certificate is issued to) and also for trust service identification.

Relying parties should verify the validity of the service certificate on receiving trust service provided using service certificate. In the case service certificate is used for qualified trust service identification, relying parties should verify certificate in accordance with an appropriate EU trusted list entry for a QTSP.

6.3.6. Certificate renewal

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

6.3.7. Certificate Re-key

Certificate re-key (issuance of a new certificate with a new public key to the same subject) may be performed only by the decision of the MitSoft QTSP.

All the practices defined for the certificate issuance are also applied for certificate re-key (see section 6.3.3).

Trust services provided by MitSoft QTSP shall use valid service certificates with a non-expired private key usage period. Therefore, MitSoft QTSP ensures regular and timely service certificate re-key, which ensures, that expired certificates or certificates with expired key usage period will not be used for service provision.

In addition to regular certificate re-key, certificate re-key is performed if:

a) certificate will expire soon or key usage period will expire soon;
b) cryptographic algorithms used are not recommended to be used after the date, which is before service certificate expiration;
c) service root CA certificate or service certificate profile was modified, due to its non-compliance with the requirements of the updated standards, legal acts, or due to MitSoft QTSP business decision;
d) data placed in the service certificate does not correspond to the legal status of trusted service;
e) certificate revocation occurs.

Issued certificates are published in the MitSoft repository.

In the case service certificate is used for qualified trust service identification, MitSoft QTSP informs Communications Regulatory Authority of the Republic of Lithuania (RRT) performing role of National Supervisory Body of qualified trust service providers about new certificate issuance for the corresponding qualified trust service provided by MitSoft QTSP. MitSoft QTSP asks RRT to initiate the procedure for including a new service certificate in the Trusted list of Lithuania. Particular trust service practice statement may define additional notifications for relying parties about issuance of the new certificate.

6.3.8. Certificate modification

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

6.3.9. Certificate revocation and suspension

MitSoft QTSP service root CA certificate or service certificate revocation can be triggered by unexpected events such as loss of the 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 QTSP.

Revocation is performed by the QTSP personnel, having trusted roles, using internal procedures.

The information about revoked service root CA certificate or service certificate is announced on the MitSoft website.

The subscribers of the trust services (provided by MitSoft QTSP) and affected by certificate revocation are also informed via contact information provided to QTSP by the subscribers of the trust services.

In the case service certificate is used for qualified trust service identification, QTSP also informs Communications Regulatory Authority of the Republic of Lithuania (RRT) performing role of National Supervisory Body of qualified trust service providers about service certificate revocation. RRT may use its own procedures to inform other relying parties about service certificate revocation.

MitSoft QTSP service root CA certificate and service certificate suspension is not applicable. Certificate is never reinstated after its revocation.

6.3.10. Certificate status services

MitSoft QTSP provides CRLs as the certificate status service. The frequency of publication of the regular CRL is at most 24 hours. Delta CRL's are not used. The nextUpdate field of the CRL indicate the latest issuance time of the next regular CRL. In the case the last CRL is issued for those certificates in the scope of the CRL, the nextUpdate field is set to "99991231235959Z".

CRLs are published in the MitSoft repository, and are publicly and internationally available for the subscribers of trust services provided by MitSoft QTSP and third parties 24 hours a day, 7 days a week. According certificate profiles, CRL distribution points extension is used, which allows subscribers and relying parties to find freshest CRL.

Fields of CRL are described in the CRL profile (section 6.6.2. CRL profiles). Revoked certificates are never removed from the CRL, even after certificates expiration.

Online Certificate Status Protocol (OCSP) is not supported.

CARL is used for publication of revocation of the service root CA certificates. CARL is issued at least once a year (with a nextUpdate of at most 1 year after the issuing date), or immediately, if service root CA certificate is revoked.

6.3.11. End of subscription

Non-applicable.

6.3.12. Key escrow and recovery

No backups of the private keys of the service root CA certificates and service certificates are created. No recovery procedures are applied for the private keys of the service root CA certificates and service certificates. On the loss of a private key, new key pair and new certificates are generated.

MitSoft QTSP trust services may define (in its practice statement) additional security measures to protect against key loss. For example (like it is done by QTSS), duplicated services with different keys may be used to ensure uninterrupted service provision.

6.4. Facility, management, and operational controls

MitSoft QTSP uses the same physical and environmental security facilities, procedural and personal controls for all provided trusted services. Practices defined in QTS PS are applied and references are provided here. Certificates issued by MitSoft QTSP CA are used by trust services provided by MitSoft QTSP and some additional controls, related to use the of certificates and environment, may be applied and defined in corresponding trust service documentation.

6.4.1. General

Refer to clauses 5, 6.3 and 7.3 of [QTS PS].

6.4.2. Physical security controls

Refer to clause 7.6 of [QTS PS].

The following controls are applied to certificate issuance service:

- [NCP+] Multiple access controls are applied to ensure the security of the cryptographic modules within physically and environmentally secure premise.

Additional physical security controls are applied for the secure cryptographic module (HSM), which holds the MitSoft QTSP Root CA keys:

- HSM is stored in a high security zone, which is physically isolated from normal operations;
- HSM is stored in a place, which has physical protection against unauthorized access;
- environmental storage conditions meet the manufacturer's requirements for the HSM;
- HSM is disconnected from network;
- only personnel in trusted roles has access to HSM;
- multiple access controls are applied to access private keys held within HSM.

6.4.3. Procedural controls

Refer to clause 7.4 of [QTS PS].

Additionally, the following practices are applied:

a) If a certificate (service root CA certificate) is issued by the MitSoft QTSP Root CA certificate, certificate issuance is performed only by trusted roles and under, at least, dual control ensured by internal procedures.

6.4.4. Personnel controls

Refer to clause 7.2 of [QTS PS].

Additionally, the following practices are applied:

a) Trusted roles are defined in the MitSoft QTSP's information security policy and include roles that involve the following responsibilities:
   - HSM security officers: authorized to create, destroy cryptographic keys and certificates, perform HSM maintenance (installs, update and

configures HSM). Responsible for generating and storing partitioned access key used for dual-control.

6.4.5. Audit logging procedures

Refer to clause 7.10 of [QTS 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 and reports of the performed actions are made.

c) Records concerning HSM failures and reports of the performed actions are made.

6.4.6. Records archival

Records concerning all events relating to the life-cycle of the issued certificates and their keys are stored at least for 7 years after certificates expiration.

6.4.7. Key changeover

Non-applicable.

6.4.8. Compromise and disaster recovery

Refer to clauses 7.9 and 7.11 of [QTS PS].

Additionally:

a) In the case of the compromise, loss, or suspected compromise of a CA's private key, CA certificate and all subordinate certificates are revoked, and relying parties are informed. The corresponding information is published on the MitSoft website.

b) Since no backup copies of the private keys are made, if CA certificate unexpectedly loss its validity, new keys are generated and new CA certificate is issued.

c) In the case any of the algorithms or associated parameters, used in issued certificate, become insufficient for certificate remaining intended usage, revocation of the certificate is scheduled and concerned third parties are informed.

d) In the case any part of the partitioned access key is lost, new partitioned access key is generated according internal dual control procedures.

6.4.9. Certification Authority or Registration Authority termination

Refer to clause 7.12 of [QTS PS].

Additionally:

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

b) In the case QTSP transfers its obligations to other party, revocation status information (CRLs and CARLs), event log archives and other information necessary to provide evidence of the operation of the QTSP are also provided.

Trust service, which uses service certificate issued by MitSoft QTSP CA, may address additional practices related to service certificate, corresponding keys and secure cryptographic devices used.

6.5. Technical security controls

Refer to clause 7.5 of [QTS PS].

6.5.1. Key pair generation and installation

Key pair and certificate generation is performed in a physically secured environment and only by trusted roles following internal MitSoft QTSP procedures.

CA certificates (MitSoft QTSP Root CA and service root CA certificates) and corresponding key pairs generation are performed only under, at least, dual control. Private keys are generated within a secure cryptographic module. Private keys are never exported from SCD and never imported into SCD.

[NCP+] If end-entity service certificate is issued under NCP+ certificate policy, key pair and certificate generation are performed only under, at least, dual control. Private keys are generated within a secure cryptographic module. Private keys are never exported from SCD and never imported into SCD.

Cryptographic algorithms, key lengths, and generation parameters for key generation and certificate issuance are selected according to recommendations of ETSI TS 119 312 and ENISA.

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 6.6.1. Certificate profiles).

QTSP service root certificates and service certificates are issued to MitSoft QTSP trust services in accordance with MitSoft trust service procedures, those ensure uninterrupted trust service provision.

6.5.2. Private key protection and cryptographic module engineering controls

Private keys for MitSoft QTSP Root CA certificates are held and used within a cryptographic module, which assure EAL4+ level or higher in accordance with ISO/IEC 15408.

[NCP+] If service root CA certificate or end-entity service certificate is issued under NCP+ certificate policy, private signing keys are held and used within a cryptographic module, which assure EAL4+ level or higher in accordance with ISO/IEC 15408.

Used secure cryptographic device is operated in its configuration as described in the manufacturer documentation, which ensures compliance to declared security assurance level. Measures are being taken to ensure that used secure cryptographic device is not tampered with during shipment and storage, and it is functioning correctly.

Backup copies of the private keys are not created.

6.5.3. Other aspects of key pair management

Private keys are not used beyond the corresponding certificate expiration. Private keys are not used beyond the end of their life cycle. Details of the used private key usage period extension are defined in the corresponding certificate profile (see section 6.6.1. Certificate profiles).

CA signing keys are used only within physically secure premises and only for subordinate certificate signing and issuing revocation status information. The corresponding key usage attributes are used within generated CA certificates (see section 6.6.1. Certificate profiles).

6.5.4. Activation data

Internal MitSoft dual control procedures, used for private keys and certificate generation) ensures, that simultaneous control of at least two trusted employees is required.

6.5.5. Computer security controls

Refer to clause 7.4 of [QTS PS].

Additionally:

a) [NCP+] Service certificates are issued in a secure environment, which requires at least dual control to be used for authentication.

6.5.6. Life cycle security controls

Refer to clauses 7.7 and 7.14 of [QTS PS]

6.5.7. Network security controls

Refer to clause 7.8 of [QTS PS].

Additionally:

a) All CA systems are maintained and protected in a secure zone.

b) [NCP+] Key generation and certificate issuance are performed being physically in a secure zone by trusted roles only, network access is not used. Systems are configured by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

c) Systems used for MitSoft QTSP Root CA certificate and its keys generation are maintained and protected in a high security zone, which is disconnected from the network.

6.5.8. Timestamping

MitSoft QTSP CA issues certificates for MitSoft qualified time-stamping service. MitSoft qualified time-stamping service practice statement [QTSS PS] describes practices applied for time stamp provision.

6.6. Certificate, CRL and OCSP profiles

6.6.1. Certificate profiles

6.6.1.1 MitSoft QTSP Root CA certificate profile

This section defines certificate profile used for MitSoft QTSP CA Root certificate – certificate on the top of the CA hierarchy.

Self-signed MitSoft QTSP Root CA certificate is used only for issuing certificates for trust services provided by MitSoft QTSP itself. MitSoft QTSP Root CA certificate profile defines X.509 version 3 certificate structure and it is conformant to RFC 5280 and ETSI EN 319 412-3.

6.6.1.1.1 Certificate fields

Certificate fields for the MitSoft QTSP Root CA certificate profile are presented in Table 4.

Table 4. Certificate fields for the MitSoft QTSP Root CA certificate profile

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 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>[1]. DN contains the following attributes: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). For example, "CN=MitSoft QTSP Root CA, 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>**Error! Bookmark not defined.**. DN contains the following attributes: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). For example, "CN=MitSoft QTSP Root CA, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"

[1] DN should be conformant to ETSI EN 319 412-3.

Not Before	Yes	Start of the certificate validity period. The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate	<Date with time>
Not After	Yes	End of the certificate validity period. The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate	<Date with time>
Signature Algorithm	Yes	Contains the algorithm identifier for the algorithm used by the CA to sign the certificate	ecdsa-with-SHA512[2] (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[2] (OID: 1.2.840.10045.2.1) with P-521 elliptic curve[3] (OID: 1.3.132.0.35)
Signature Value	Yes	Contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate field	

6.6.1.1.2 Certificate extensions

Certificate extensions for the MitSoft QTSP Root CA certificate profile are presented in Table 5.

Table 5. Certificate extensions for the MitSoft QTSP Root CA certificate profile

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: None
Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key contained in the certificate	keyCertSign (5), cRLSign (6)

[2] References to algorithm descriptions are presented in ETSI TS 119 312.
[3] Elliptic Curves are defined in RFC 5480.

6.6.1.2 MitSoft QTSA CA certificate profile

MitSoft QTSP provides Qualified Time-stamping service, which uses 2 Time-Stamping Units (TSUs). This section defines certificate profile used for CA certificates, that are used as root certificates for MitSoft Qualified Time-stamping service.

MitSoft QTSA CA certificates are used only for issuing TSU certificates and corresponding CRLs signing. MitSoft QTSA CA certificates are issued under NCP+ (Normalized Certificate Policy requiring a secure cryptographic device) certificate policy defined in ETSI EN 319 411-1. Private keys of the MitSoft QTSA CA certificate reside in a HSM dedicated to TSU to which this certificate was issued (see [QTSS PS] for details).

MitSoft QTSA CA certificate profile defines X.509 version 3 certificate structure and it is conformant to RFC 5280 and ETSI EN 319 412-3.

6.6.1.2.1 Certificate fields

Certificate fields for the MitSoft QTSA CA certificate profile are presented in Table 6.

Table 6. Certificate fields for the MitSoft QTSA CA certificate profile

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 CA 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>[4]. DN contains the following attributes: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). For example, "CN=MitSoft QTSP Root CA, 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>**Error! Bookmark not defined.**. DN contains the following attributes: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). For example, "CN=MitSoft QTSA TSU-1 CA, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"

[4] DN should be conformant to ETSI EN 319 412-3.

Not Before	Yes	Start of the certificate validity period. The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate	<Date with time>
Not After	Yes	End of the certificate validity period. The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate	<Date with time>
Signature Algorithm	Yes	Contains the algorithm identifier for the algorithm used by the CA to sign the certificate	ecdsa-with-SHA512[5] (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[2] (OID: 1.2.840.10045.2.1) with P-521 elliptic curve[6] (OID: 1.3.132.0.35)
Signature Value	Yes	Contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate field	

6.6.1.2.2 Certificate extensions

Certificate extensions for the MitSoft QTSA CA certificate profile are presented in Table 7.

Table 7. Certificate extensions for the MitSoft QTSA CA certificate profile

Extension	Required	Critical	Description	Possible values
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)	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

[5] References to algorithm descriptions are presented in ETSI TS 119 312.
[6] Elliptic Curves are defined in RFC 5480.

Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key contained in the certificate	keyCertSign (5), cRLSign (6)
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: 0.4.0.2042.1.2 (NCP+ certificate policy), 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>

6.6.1.3 MitSoft QTSA TSU certificate profile

MitSoft QTSP provides Qualified Time-stamping service, which uses 2 Time-Stamping Units (TSUs). This section defines certificate profile used for TSU certificates, that are used as end-entity certificates for MitSoft Qualified Time-stamping service.

MitSoft QTSA TSU certificates are used only for signing qualified time stamps issued by MitSoft Qualified Time-stamping service. MitSoft QTSA TSU certificates are issued under NCP+ (Normalized Certificate Policy requiring a secure cryptographic device) certificate policy defined in ETSI EN 319 411-1. Private keys of the MitSoft QTSA TSU certificate reside in a HSM dedicated to TSU to which this certificate was issued (see [QTSS PS] for details). The MitSoft QTSA TSU certificate profile is aligned with the requirements defined in ETSI EN 319 422.

MitSoft QTSA TSU certificate profile defines X.509 version 3 certificate structure and it is conformant to RFC 5280, ETSI EN 319 412-3 and ETSI EN 319 422.

6.6.1.3.1 Certificate fields

Certificate fields for the MitSoft QTSA TSU certificate profile are presented in Table 8.

Table 8. Certificate fields for the MitSoft QTSA TSU certificate profile

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 CA 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>[7]. DN contains the following attributes: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). For example, "CN=MitSoft QTSA TSU-1 CA, 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> **Error! Bookmark not defined.** DN contains the following attributes: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). For example, "CN=MitSoft QTSA TSU-1, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"

[7] DN should be conformant to ETSI EN 319 412-3.

Not Before	Yes	Start of the certificate validity period. The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate	<Date with time>
Not After	Yes	End of the certificate validity period. The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate	<Date with time> Not After = Not Before + 2740 days
Signature Algorithm	Yes	Contains the algorithm identifier for the algorithm used by the CA to sign the certificate	ecdsa-with-SHA512[8] (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[9] (OID: 1.3.132.0.34)
Signature Value	Yes	Contains a digital signature computed upon the ASN.1 DER encoded tbsCertificate field	

6.6.1.3.2 Certificate extensions

Certificate extensions for the MitSoft QTSA TSU certificate profile are presented in Table 9.

Table 9. Certificate extensions for the MitSoft QTSA TSU certificate profile

Extension	Required	Critical	Description	Possible values
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

[8] References to algorithm descriptions are presented in ETSI TS 119 312.
[9] Elliptic Curves are defined in RFC 5480.

Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key contained in the certificate	digitalSignature (0)
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: 0.4.0.2042.1.2 (NCP+ certificate policy), 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

6.6.2. CRL profiles

6.6.2.1 Profile of the CARL for MitSoft QTSA CA certificates

MitSoft Certificate Authority Revocation Lists for MitSoft QTSA CA certificates are issued in accordance with RFC 5280.

6.6.2.1.1 CARL fields

Fields for the CARL profile for MitSoft QTSA CA certificates are presented in Table 10.

Table 10. Fields for the CARL profile for MitSoft QTSA CA 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[10] (OID: 1.2.840.10045.4.3.4)
Issuer Name	Yes	Identifies the entity that has signed and issued the CRL	<Issuer distinguished name>[11]. DN contains the following attributes: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). For example, "CN=MitSoft QTSP Root CA, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
This Update	Yes	Indicates the issue date of this CRL	<Date with time>
Next Update	Yes	Indicates the date by which the next CRL will be issued	<Date with time>
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: • Certificate serial number, • Revocation date, • Revocation reason code according to RFC 5280

[10] References to algorithm descriptions are presented in ETSI TS 119 312.
[11] DN should be conformant to ETSI EN 319 412-3.

6.6.2.1.2 CARL extensions

Extensions for the CARL for MitSoft QTSA CA certificates profile are presented in Table 11.

Table 11. CRL extensions for the CARL profile for MitSoft QTSA CA certificates

Extension	Required	Critical	Description	Possible values
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, CA 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: True; indirectCRL: False; onlyContainsAttributeCerts: 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>

6.6.2.2 Profile of the CRL for MitSoft QTSA TSU certificates

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

6.6.2.2.1 CRL fields

CRL fields for the CRL profile for MitSoft QTSA TSU certificates are presented in Table 12.

Table 12. Fields for the CRL profile for MitSoft QTSA 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[12] (OID: 1.2.840.10045.4.3.4)

[12] References to algorithm descriptions are presented in ETSI TS 119 312.

Issuer Name	Yes	Identifies the entity that has signed and issued the CRL	<Issuer distinguished name>[13]. DN contains the following attributes: • C (countryName), • O (organizationName), • 2.5.4.97 (organizationIdentifier), • CN (commonName). For example, "CN=MitSoft QTSA TSU-1 CA, O=MitSoft, organizationIdentifier= NTRLT-120792080, C=LT"
This Update	Yes	Indicates the issue date of this CRL	<Date with time>
Next Update	Yes	Indicates the date by which the next CRL will be issued	<Date with time>
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: • Certificate serial number, • Revocation date, • Revocation reason code according to RFC 5280

6.6.2.2.2 CRL extensions

Extensions for the CRL for MitSoft QTSA TSU certificates profile are presented in Table 13.

Table 13. CRL extensions for the CRL profile for MitSoft QTSA TSU certificates

Extension	Required	Critical	Description	Possible values
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>

[13] DN should be conformant to ETSI EN 319 412-3.

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, CA 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; onlyContainsAttributeCerts: 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>

6.6.3. OCSP profiles

Non-applicable.

6.7. Compliance audit and other assessment

Refer to clause 7.13 of [QTS PS].

Additionally:

a) QTSP confirms that the MitSoft QTSP internal CA conform to this Certification Practice Statement.

6.8. Other business and legal matters

6.8.1. Fees

Non-applicable.

6.8.2. Financial responsibility

Refer to clause 7.1.1 of [QTS PS].

6.8.3. Confidentiality of business information

Non-applicable.

6.8.4. Privacy of personal information

Refer to clause 7.13 of [QTS PS].

Additionally:

a) MitSoft QTSP CA does not collect and does not store any data (including personal data) of the subscribers/subjects, since it issues certificates only for MitSoft QTSP trusted services.

6.8.5. Intellectual property rights

Refer to clause 6.1.1.5 of [QTS PS].

6.8.6. Representations and warranties

MitSoft QTSP CA provide all its certification services consistent with this CPS.

6.8.7. Disclaimers of warranties

Non-applicable.

6.8.8. Limitations of liability

Refer to clause 6.1.1.2 of [QTS PS].

6.8.9. Indemnities

Non-applicable.

6.8.10. Term and termination

Refer to clause 7.12 of [QTS PS].

Additionally:

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

b) Every issued non-expired end-entity certificate is revoked.

6.8.11. Individual notices and communications with participants

Non-applicable.

6.8.12. Amendments

Void.

6.8.13. Dispute resolution procedures

Refer to clause 6.1.1.3.2 of [QTS PS].

6.8.14. Governing law

Refer to clause 6.1.1.3.1 of [QTS PS].

6.8.15. Compliance with applicable law

Refer to clause 7.13 of [QTS PS].

6.8.16. Miscellaneous provisions

Non-applicable.

6.9. Other provisions

6.9.1. Organizational

Refer to clause 7.1 of [QTS PS].

Additionally:

a) Certificates and private key generation and certificate revocation are performed by HSM security officers under the MitSoft director's decision and order. Impartiality is determined by the fact that MitSoft QTSP CA issues certificates only to MitSoft QTSP itself.

b) Any staff in trusted roles involved into certificate generation and revocation management are free from any commercial, financial, and other pressures which might adversely influence trust in the provided service

6.9.2. Additional testing

MitSoft QTSP CA does not issue certificates for external subscribers or subjects. Therefore, third party certificate testing covers only certificate validation testing in the context of the provided trust services and does not cover private key usage or certificate revocation.

All the certificates issued by the MitSoft QTSP CA are publicly and freely available on the MitSoft repository. This allows any third party to check and test every certificate issued by MitSoft QTSP CA.

6.9.3. Disabilities

Non-applicable.

6.9.4. Terms and conditions

Refer to clause 6.2 of [QTS PS].

Additionally, the terms and conditions of MitSoft QTSP CA certification service specify the following:

a) Information on how to verify certificates and their revocation, and any possible limitations on the certificate usage.

Terms and conditions of the MitSoft certification service is not presented as separate document, but it is an integral part of this CPS document (see section 4.2.3 Terms and conditions and PKI disclosure statement).