mitsoft

Qualified Time-Stamping Service

Time-Stamping Practice Statement

QTSS/PS

Unique object ID (OID): **1.3.6.1.4.1.57890.1.3.1**

Version 1.10

Valid since 2026-09-01

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	2024-10-01	First official version of the document
1.10	2026-09-01	Updated according to new requirements

Approval of the document

	Name	Date	Signature
Reviewed by	Adomas Birštunas	2026-05-28	
Approved by	Antanas Mitašiūnas	2026-05-29	

Table of content

1. INTRODUCTION 5
1.1. Overview 5
1.2. Identification 6
1.3. Users and fields of application of the time-stamping service 6
1.4. Conformance. Its confirmation and verification 6
1.5. Contact information 6
2. References 8
3. Definitions of terms and abbreviations 9
4. MitSoft TSA: General Concepts 11
5. Introduction to time-stamp policies 12
6. POLICIES AND PRACTICES 13
6.1. Risk assessment 13
6.2. Time-stamping service practice statement 13
6.3. Terms and conditions 13
6.4. Information security policy 13
6.5. TSA obligations 14
6.5.1. General 14
6.5.2. TSA obligations towards subscribers 14
6.5.3. Subscriber obligations 14
6.5.4. Intellectual property rights 14
6.5.5. Liability 14
6.5.6. Legal provisions and interpretations 14
6.6. Information for relying parties 14
7. TSA MANAGEMENT AND OPERATION 15
7.1. Introduction 15
7.2. Internal organization 15
7.3. Personnel security 15
7.4. Asset management 15
7.5. Access control 15
7.6. Cryptographic controls 15
7.6.1. General 15
7.6.2. TSU key generation 15
7.6.3. TSU private key protection 16
7.6.4. TSU public key certificate 16
7.6.5. Rekeying TSU's key 16
7.6.6. Life cycle management of signing cryptographic hardware 17
7.6.7. End of TSU key life cycle 17
7.7. Time-stamping 18

7.7.1. Time-stamp issuance 18
7.7.2. Clock synchronization with UTC 20
7.8. Physical and environmental security 20
7.9. Operation security 20
7.10. Network security 21
7.11. Incident management 21
7.12. Collection of evidence 21
7.13. Business continuity management 21
7.14. TSA termination and termination plans 21
7.15. Compliance 21
7.16. Supply chain 21
8. ADDITIONAL REQUIREMENTS FOR QUALIFIED ELECTRONIC TIME-STAMPS AS PER REGULATION (EU) No 910/2014 22
8.1. TSU public key certificate 22
8.2. TSU issuing non-qualified and qualified electronic time-stamps as per Regulation (EU) No 910/2014 22

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 has divided its Practice Statements into three parts:

- Qualified Trust Services Practice Statement (QTS PS) describes general practices common to all qualified trust services;
- Preservation Practice Statement (QLPS PS) and Time-Stamping Practice Statement (QTSS PS) describe parts that are specific to each qualified service.

1.1. Overview

The standard ETSI EN 319 421 "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-stamps" specifies Qualified Time-stamps policy: a Best practices Time-Stamp Policy (BTSP) for TSAs issuing time-stamps, supported by public key certificates, with an accuracy of 1 second or better time-stamping service policy (OID: 0.4.0.2023.1.1). The requirements specified in the policy 0.4.0.2023.1.1 are related neither to concrete technological solutions nor to the organizational structure of the Time-Stamping Authority (TSA) – trust service provider providing time-stamping services using one or more time-stamping units. Technical solutions, procedures, and personnel policy for the implementation of the policy 0.4.0.2023.1.1 requirements are described in the present MitSoft Qualified Time-Stamping Service Practice Statement (further – QTSS PS).

The present QTSS PS 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 [eIDAS];

b) Commission implementing Regulation (EU) 2025/1929 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the binding of date and time to data and establishing the accuracy of the time sources for the provision of qualified electronic time stamps;

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

d) ETSI EN 319 421: "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing qualified time-stamps";

e) ETSI EN 319 422 "Electronic Signatures and Infrastructures (ESI); Time-stamping Protocol and time-stamp token profiles";

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

g) Council of the Communications Regulatory Authority of the Republic of Lithuania, Resolution No. TN-276, On the Approval of the Description of the Procedure for Granting the Status of a Qualified Trust Service Provider and the Performance of Certain Operational Requirements (June 23, 2026).

While providing the time-stamping service, TSP carries out the functions of generation of time data in electronic form which binds other electronic data to particular time establishing evidence that these data existed at that time.

Note regarding the definitions. Time stamps means qualified electronic time stamps as per Regulation (EU) No 910/2014 [eIDAS]. Qualified Time-Stamping Service Policy means a Best practices Time-Stamp Policy (BTSP) with OID 0.4.0.2023.1.1.

Terms and Conditions of MitSoft Time-Stamping Authority meets the requirements for Disclosure Statement defined in ETSI EN 319 421.

1.2. Identification

The unique identifier (OID) of the QTSS PS is 1.3.6.1.4.1.57890.1.3.1; the values of its fields are given in the Table 1.

Table 1. The values of the fields of the unique identifier of the QTSS PS

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: Qualified Time-Stamping Service Practice Statement	3
Document version	1

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

1.3. Users and fields of application of the time-stamping service

Qualified time-stamping service provides means to guarantee the proof of existence for the data - evidence that proves that data existed at a specific time and has not been altered. The users of the qualified time-stamping service provided by the TSA can be legal or natural persons needing the services provided by the TSA.

Neither BTSP nor QTSS PS imposes any limitations for using the Qualified Time-Stamping Service. It can be used when a signatory or signing service providers want to capture the time and protect the data from alteration.

TSA provides public services; however, it can also serve closed user groups.

1.4. Conformance. Its confirmation and verification

TSA confirms that the MitSoft Time-Stamping Service is EU qualified time-stamping service and conforms to the BTSP.

The compliance of the TSA's activities with the BTSP and QTSS PS is verified as defined by the QTSS PS, at least every two years.

1.5. Contact information

The QTSS PS is managed by the joint stock company "MIT-SOFT", which contact information is given in the Table 2.

Table 2. Contact information of the TSA

TSA:	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.

[CIR2025/1929] – Commission implementing Regulation (EU) 2025/1929 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the binding of date and time to data and establishing the accuracy of the time sources for the provision of qualified electronic time stamps.

[ENISA] – Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by 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 319 421] – ETSI EN 319 421 Electronic Signatures and Trust 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 3161] – RFC 3161: Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP).

[RFC 5816] – RFC 5816: ESSCertIDv2 Update for RFC 3161.

[TS 119 312] – ETSI TS 119 312 "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites" standard.

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

[CS CPS] - MitSoft "Certification Service. Certification Practice Statement".

3. Definitions of terms and abbreviations

Certificate validity period: time interval (notBefore and notAfter inclusive) during which the Certification Authority (CA) warrants that it will maintain information about the status of the certificate

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].

EU qualified time-stamping authority: qualified trust-service provider issuing qualified electronic time stamps as laid down in Regulation (EU) No 910/2014 [eIDAS].

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.

Leap second: adjustment to UTC by skipping or adding an extra second on the last second of a UTC month.

Proof of existence: evidence that proves that an object existed at a specific date/time.

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.

Secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user.

Signer: entity being the creator of a digital signature.

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-stamp policy: named set of rules that indicates the applicability of a time stamp to a particular community and/or class of application with common security requirements.

Time-stamp token: data object defined in IETF RFC 3161, representing a time stamp.

Time-stamp users: recipients (including subscribers) of the time stamps who rely upon them.

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 Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements.

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].

TSA system: composition of IT products and components organized to support the provision of time-stamping services.

UTC(k): time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.

BIPM – Bureau International des Poids et Mesures
BTSP – Best practice Time-Stamp Policy
ESI – Electronic Signature and Infrastructure
ETSI – European Telecommunications Standards Institute
OID – Object identifier
OVR – General Requirement
PS - Practice Statement
QLPS – Qualified Long-term Preservation Service
QTS - Qualified Trust Services
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 TSA: General Concepts

The definition of qualified time-stamping service by ETSI EN 319 421 consists of two types of requirements: generic policy requirements common to all classes of trust service providers services defined by ETSI EN 319 401 and service's topic-oriented requirements targeted to the definition of qualified time-stamping specific service requirements by ETSI EN 319 421 and qualified time stamp token definition profiled by ETSI EN 319 422.

The provision of time-stamping services is divided into the following component services for the purposes of classifying requirements:

1) Time-stamping provision: This service component generates time stamps.
2) Time-stamping management: This service component monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the time-stamping provision service.

This subdivision of services places no restrictions on any subdivision of an implementation of time-stamping services.

5. Introduction to time-stamp policies

Legal requirements for Trust Service Providers (TSP) providing services to the public, including TSPs issuing time stamps are provided by the Regulation. More specific requirements are identified in the Regulation for a specific class of TSP called a Qualified TSP, with further specific requirements for those Qualified TSPs which issue qualified time stamps. This time stamps policy is aimed to meet the requirements of the Regulation for Qualified TSPs issuing Qualified electronic time stamps respectively.

In order to verify an electronic signature, it can be necessary to prove that the signature from the signer was applied when the signer's certificate was valid. The trustworthy time obtained from the trusted service provider is necessary. Such a trustworthy time may be provided as a time stamp. Time stamps may also be applied in other applications, where the proof that a datum existed before a particular time is needed.

Time-stamping is gaining an increasing interest by the business sector and is becoming an important component of digital signatures, this is commonly based upon the Time-Stamp protocol from the IETF RFC 3161 which is profiled in ETSI EN 319 422. Agreed minimum security and quality requirements are necessary in order to ensure trustworthy validation of long-term digital signatures or other time stamp applications.

Time stamp policy defines named set of rules that indicates the applicability of a time stamp to a particular community and/or class of application with common security requirements.

The TSA includes the identifier for the time-stamp policies being supported in the Terms and Conditions that the TSA makes available to subscribers and relying parties, to indicate its claim of conformance.

The TSA supports and includes the below defined BTSP identifier in the time-stamp policy and in the TSA Terms and Conditions that the TSA makes available to subscribers and relying parties, to indicate its claim of conformance.

6. POLICIES AND PRACTICES

6.1. Risk assessment

Refer to clause 5 of [QTS PS].

6.2. Time-stamping service practice statement

Refer to clause 6.1 of [QTS PS].

Additionally, for providing qualified time-stamping services:

a) The practices and procedures used to address the requirements identified in the BTSP time-stamping policy (OID: 0.4.0.2023.1.1) are described in the present Time-Stamping Service Practice Statement (QTSS PS).

b) The information about the availability of its time stamping service is described in TSA Terms and Conditions.

c) The QTSS PS identifies the obligations of all external organizations supporting the TSA services including the applicable policies and practices.

BTSP is the only qualified trust service policy supported by the MitSoft TSA:

a) Hashing algorithms that can be used to represent the datum being time-stamped and the accuracy of the time in the time-stamps with respect to UTC are specified in the section 7.7.1. Time-stamp issuance.

b) The subscriber obligations are specified in the section 6.5.3. Subscriber obligations.

c) The relying party obligations are specified in the section 6.6. Relying party obligations.

d) The time-stamping service of qualified time stamps is qualified time-stamping service as per Regulation (EU) No 910/2014 [eIDAS]. TSA operates in the Republic of Lithuania and follows EU and Lithuanian laws and normative legal acts.

Disclosure statement of MitSoft TSA is specified in Terms and Conditions of its Qualified Time-Stamping Service.

6.3. Terms and conditions

Refer to clause 6.2 of [QTS PS].

Additionally, the terms and conditions of qualified time-stamping service specify the following:

a) The BTSP being applied.

b) Information on how to verify the time stamps, and any possible limitations on the validity period associated with it.

c) Information about the availability of its time stamping service.

d) Whether the qualified time-stamping service has been assessed to be conformant with the BTSP, and if so through which conformity assessment scheme.

6.4. Information security policy

Refer to clause 6.3 of [QTS PS].

6.5. TSA obligations

6.5.1. General

The TSA ensures that all requirements on TSA are implemented as applicable to the BTSP. TSA ensures implementation of the following:

a) Procedures defined in the present QTSS PS, including the services of time stamps generation and management;

b) Adherence to any additional obligations either indicated in the Terms and conditions or incorporated by reference;

c) Certificate revocation lists (CRLs) for TSU certificates are updated and this information is continuously available (for details, see [CS CPS], section 6.3.10. Certificate status services);

d) Issued time stamp tokens claim to be qualified electronic time stamps and contain corresponding extension (for details, see the section 7.7.1. Time-stamp issuance).

6.5.2. TSA obligations towards subscribers

Refer to clause 6.1.1.1 of [QTS PS].

6.5.3. Subscriber obligations

When relying upon a qualified time stamp, the subscriber shall verify that the time stamps has been correctly created (for details, see the section 6.6. Information for Relying parties).

6.5.4. Intellectual property rights

Refer to clause 6.1.1.5 of [QTS PS].

6.5.5. Liability

Refer to clause 6.1.1.2 of [QTS PS].

6.5.6. Legal provisions and interpretations

Refer to clause 6.1.1.3 of [QTS PS].

6.6. Information for relying parties

The relying party, when relying upon a qualified time stamp, shall verify that the qualified time stamp has been correctly signed and that the private key used to sign the time stamp has not been compromised (disclosed to third-parties or unusable for other reasons) until the time of verification.

The time stamp is verified during the TSU's certificate validity period; therefore, the validity of the signing key can be checked by making sure that the TSU's certificate has not been revoked. Indications on verification of time stamp tokens is specified in Terms and Conditions of Qualified Time-Stamping Service.

Besides that, the relying party shall comply with the constraints on the use of the time-stamping service defined in the BTSP and take any other measures of precaution.

7. TSA MANAGEMENT AND OPERATION

7.1. Introduction

TSA may set the prices for its qualified time-stamping services. The TSA follows all the practices indicated in the following clauses.

7.2. Internal organization

Refer to clause 7.1 of [QTS PS].

7.3. Personnel security

Refer to clause 7.2 of [QTS PS].

Trusted roles are defined in the MitSoft QTSP's information security policy, including HSM security officer role that involve the following responsibilities:

- HSM security officer is authorized to create, destroy cryptographic keys and certificates, perform HSM maintenance (installs, update and configures HSM), is responsible for generating and storing partitioned access key used for dual-control.

7.4. Asset management

Refer to clause 7.3 of [QTS PS].

7.5. Access control

Refer to clause 7.4 of [QTS PS].

7.6. Cryptographic controls

7.6.1. General

The TSA ensures the security of cryptographic keys and cryptographic devices throughout their lifecycle as detailed in the following clauses.

7.6.2. TSU key generation

The TSA generates its cryptographic keys under controlled circumstances. In particular:

a) The generation of the TSU's signing key(s) is carried out within a secure cryptographic device which is a trustworthy system certified in accordance with Common Criteria for Information Technology Security Evaluation, as set out in ISO/IEC 15408, and certified to EAL 4 or higher.

b) Secure cryptographic device is configured and used in accordance with device documentation and its certification.

c) The generation of the TSU's signing key(s) is undertaken in a physically secured environment by personnel in trusted roles (see clause 7.6.2. of [EN 319 421]) under, at least, dual control. The personnel authorized to carry out this function are limited to those required to do so under the TSA's practices.

d) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps and for signing TSU public key certificates respectively are compliant with ETSI TS 119 312 and the

Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA.

e) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time stamp tokens key are recognized as being suitable for the purposes of time stamp tokens issued by the TSA. Particular signing algorithms and key lengths used for time stamp creation are defined in the TSU certificate profiles (see [CS CPS], section 6.6.1.3. MitSoft QTSA TSU certificate profile.

f) A TSU's signing key is generated within cryptographic module and never exported from it, and never imported into it.

g) A TSU has a single time stamp signing key active at a time.

7.6.3. TSU private key protection

The TSA ensures that TSU private keys remain confidential and maintains their integrity. In particular:

a) The TSU private key is held and used within a secure cryptographic device which is a trustworthy system certified in accordance with Common Criteria for Information Technology Security Evaluation, as set out in ISO/IEC 15408, and certified to EAL 4 or higher.

b) TSU's private keys are created within cryptographic module and never leave it. TSU's private keys generation is performed only by personnel in trusted roles using, at least, dual control in a physically secured environment, in a premise protected from unattended access (see clause 7.6.3. of [EN 319 421]). The personnel authorized to carry out this function are limited to those who are required to do so under the TSA's practices.

c) No backup copies of the TSU's private keys are created.

7.6.4. TSU public key certificate

The TSA ensures that the integrity and authenticity of the TSU signature verification (public) keys and any associated parameters are maintained during its distribution to relying parties. In particular:

a) TSU signature verification (public) keys are made available to relying parties in public key certificates.

b) The signature verification (public) key certificate used by TSU is issued by a certification authority operating under ETSI EN 319 411-1 standard. TSU certificates are issued under NCP+ (Normalized Certificate Policy requiring a secure cryptographic device) certificate policy (OID 0.4.0.2042.1.2), which is defined in the standard ETSI EN 319 411-1 (see [CS CPS] for details).

c) The TSU cannot issue time stamps before the corresponding signature verification (public key) certificate is loaded into it.

TSU certificate profile is defined in the Certification Practice Statement of the Certification Service of the MitSoft TSP internal CA [CS CPS] (section 6.6.1.3. MitSoft QTSA TSU certificate profile) and ensures alignment with requirements defined in ETSI EN 319 422.

7.6.5. Rekeying TSU's key

To address cryptographic security requirements and to reduce an impact of algorithm weakening or key compromises, rekeying of TSU's keys is performed every two years, using algorithm and key length that is recognized to be suitable for a period of at least 5 years.

To account for procedures of certification and certificate inclusion in the Trusted list, the validity of signing keys is limited to 3 years. The certificates include the

extension indicating the corresponding Private key usage period.

To allow for a sufficient period of time of the validity of time stamps, the validity of TSU's certificates is set to 7.5 years. If it appears that the algorithms used are becoming unsuitable for this period, the affected certificates are revoked.

The exact periods of private key usage and certificate validity are defined in the TSU certificate profile (see [CS CPS], section 6.6.1.3. MitSoft QTSA TSU certificate profile).

7.6.6. Life cycle management of signing cryptographic hardware

The TSA ensures the security of cryptographic hardware throughout its lifecycle. In particular, the TSA ensures that:

a) Time stamp token signing cryptographic hardware is not tampered with during shipment and while stored. Prior to installation, the hardware has been checked by security officers in accordance with the information security policy, and the results are documented in the journal of the hardware unit.

b) Generation and activation of TSU's signing keys in cryptographic hardware is done only by personnel in trusted roles using, at least, dual control in a physically secured environment. These events are recorded in the journal of the hardware unit. Backup of keys is not performed.

c) TSU private signing keys stored on TSU cryptographic module are erased upon device retirement using the secure zeroization procedure described in the documentation of the device so, that it is practically impossible to recover them.

7.6.7. End of TSU key life cycle

The TSA defines an expiration date for TSU's keys. The expiration date for TSU's private keys is not later than the notAfter date of the associated TSU public key certificate validity period. The validity period of TSU keys is defined in the TSU Certificate profile (see [CS CPS], section 6.6.1.3. MitSoft QTSA TSU certificate profile). The expiration date for TSU´s private and public keys takes into account the lifetime defined in 'recommended key sizes versus time' from ETSI TS 119 312 and is compliant with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA. The expiration date of a key is set during key generation and included in the TSU's public key certificate.

The TSA ensures that TSU private signing keys are not used beyond the end of their validity period. In particular:

a) A new key pair is generated every two years, one year before the defined expiration date of the previous one, following the appropriate procedures (see section 7.6.2. TSU key generation). The corresponding public key certificate is generated and procedures for its inclusion in the Trusted list of Lithuania are initiated (see [CS CPS], section 6.3.7. Certificate Re-key). Soon after the new certificate is included in the Trusted list, the new signing key is activated, automatically deactivating the old one, as the TSU can only have one signing key active at a time.

b) The deactivated signing key is destroyed following the appropriate procedures, so that it cannot be retrieved.

c) In order to be able to verify during a sufficient lapse of time the validity of the time-stamps, the validity of the TSU's private keys are shorter than the associated TSU public key certificate validity period. The expiration date for TSU's private key is defined by setting a privateKeyUsagePeriod extension within the TSU's public key certificate and ensured by configuring end date of the private key within HSM (if supported).

d) The TSU's private and public keys expiration dates are defined in this Practice statement (see section 7.6.5. Rekeying TSU's key).

7.7. Time-stamping

7.7.1. Time-stamp issuance

MitSoft Qualified Time-Stamping Service issues qualified electronic time stamps as per Regulation (EU) No 910/2014 [eIDAS] only.

The TSA ensures that time stamps are issued securely and include the correct date and time. In particular:

a) The time values the TSU uses in the time stamps are traceable to at least one of the real time values distributed by a UTC(k) laboratory.

b) The value of time included in the time stamp does not differ from UTC more than the accuracy defined by the TSA and in the time stamp itself.

c) If the time stamp provider's clock is detected (see the section 7.7.2 Clock synchronization with UTC) as being out of the stated accuracy, then time stamps are not issued.

d) The time stamps are signed using a key generated exclusively for this purpose.

e) The time stamp generation system rejects any attempt to issue a time stamp if the signing private key has expired.

The time stamps issued conform to the time stamp profile defined in ETSI EN 319 422. The structure of the generated time stamps is conformant to RFC 3161 and updates defined in RFC 5816.

The time-stamping server supports the time-stamping protocol via HTTPS and HTTP as defined in clause 3.4 of RFC 3161.

The list of the hash algorithms used to hash the information to be time-stamped and supported by the time-stamping service are presented in Table No. 3. Supported hash algorithms are compliant with recommendations presented in [TS 119 312] and [ENISA].

Hash algorithms used to hash the information to be time-stamped and time stamp token signature algorithms and key lengths are compliant with recommendations presented in [TS 119 312] and [ENISA] (see section 6.6.1.3. MitSoft QTSA TSU certificate profile).

Signature algorithms, key lengths and hash algorithms of the TSU certificate signature are compliant with recommendations presented in [TS 119 312] and [ENISA] (see section 6.6.1.2. MitSoft QTSA Root certificate profile).

The structure of a time stamp request accepted by the TSA is given in the Table No. 3; the structure of a time stamp issued by the TSA is given in the Table No. 4.

Table 3. The structure of a time stamp request

Field	Required	Description	Value
version	Yes	Describes the version of the Time stamp request	1

messageImprint	Yes	Contains the hash of the datum to be time-stamped	A hash algorithm OID and the hash value of the data to be time-stamped; the following algorithms supported: • SHA-256 (OID: 2.16.840.1.101.3.4.2.1)[1] • SHA-384 (OID: 2.16.840.1.101.3.4.2.2) • SHA-512 (OID: 2.16.840.1.101.3.4.2.3) • SHA3-256 (OID: 2.16.840.1.101.3.4.2.8) • SHA3-384 (OID: 2.16.840.1.101.3.4.2.9) • SHA3-512 (OID: 2.16.840.1.101.3.4.2.10)
reqPolicy	No	Indicates the TSA policy under which the TimeStampToken should be provided	If specified, shall be 0.4.0.2023.1.1[2]
nonce	No	Allows the client to verify the timeliness of the response when no local clock is available	If specified, the same value will be included in the time stamp
certReq	No	Indicates whether the certificate should be included in the time stamp	If present and set to true, the certificate of the corresponding TSU will be included in the time stamp
extensions	No	Additional information to the request	If present, should be marked as non-critical

Table 4. The structure of a time stamp

Field	Required	Description	Value
version	Yes	Describes the version of the time stamp token	1
policy	Yes	Indicate the TSA's policy under which the response was produced	OID: 0.4.0.2023.1.1[3]
messageImprint	Yes	Contains the hash of the datum to be time-stamped	Equals to the value of the corresponding field of time stamp request (TimeStampReq)
serialNumber	Yes	An integer assigned by the TSA to each TimeStampToken	An integer (up to 160 bits long), unique for every time stamp issued by the TSU
genTime	Yes	The time at which the time stamp token has been created by the TSA	UTC time indicating the time when the time stamp was created. May include fraction-of-second
accuracy	No	Represents the time deviation around the UTC time	0.5 s (500 ms)
ordering	No	The ordering of the time stamps	Not presented

[1] References to algorithm descriptions are presented in [TS 119 312] and [ENISA].
[2] Best practices policy for time-stamp defined in [EN 319 421].
[3] Best practices policy for time-stamp defined in [EN 319 421].

nonce	No	Allows the client to verify the timeliness of the response when no local clock is available	Equals to the value of the corresponding field of request (TimeStampReq), if included
tsa	No	Gives a hint in identifying the name of the TSA	Corresponds to the value of the Subject DN field of the TSU certificate used for signing the time stamp. For example, "CN=MitSoft QTSA TSU-1, O=MitSoft, organizationIdentifier=NTRLT-120792080, C=LT"
extensions	No	Additional information to the response	Indication that this time stamp token is issued as a qualified electronic time stamp according to the Regulation (EU) No 910/2014: qcStatements=esi4-qtstStatement-1

7.7.2. Clock synchronization with UTC

The TSA ensures that its clock is synchronized with UTC within the declared accuracy. In particular:

a) The clocks of TSUs are continuously synchronized with UTC by means of comparisons to the time disseminated by UTC(k) laboratories, published in the "Circular T" of the Bureau International des Poids et Mesures (BIPM), and adjustments. The time of the clocks is traceable to UTC through a chain of comparisons, uncertainty of which is within the declared accuracy.

b) The TSU clocks are protected against threats, including tampering by unauthorized personnel, radio or electrical shocks, that could result in an undetected change to a clock that could take it outside its calibration.

c) The systems used by the TSA are capable to detect if the time that would be indicated in a time stamp drifts or jumps out of synchronization with UTC.

d) If it is detected that the time that would be indicated in a time stamp drifts or jumps out of synchronization with UTC, the time stamp issuance is stopped.

e) The TSU clocks maintain synchronization when a leap second occurs as notified by the appropriate body. The change to take account of the leap second occurs during the last minute of the day when the leap second is scheduled to occur. The systems record the exact time of this change. If a leap second is inserted, to prevent ambiguity and problems for the systems that cannot handle 61 seconds per minute, time stamps are not issued during the leap second and the second before it.

7.8. Physical and environmental security

Refer to clause 7.6 of [QTS PS].

The following controls are applied to qualified time-stamping service:

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

7.9. Operation security

Refer to clause 7.7 of [QTS PS].

7.10. Network security

Refer to clause 7.8 of [QTS PS].

Additionally:

a) TSU systems are treated as critical QTSP systems and, as such, are maintained and protected in a secure zone. Network access to time-stamping services provided by the TSU systems is possible though security appliances and dedicated reverse proxy servers only.

b) To ensure a high level of availability of external access to the time-stamping service, it has redundant external network connections.

7.11. Incident management

Refer to clause 7.9 of [QTS PS].

7.12. Collection of evidence

Refer to clause 7.10 of [QTS PS].

Additionally:

a) Records concerning all events relating to the life-cycle of TSU keys and TSU certificates are logged.

b) Records concerning all events relating to synchronization of a TSU's clock to UTC are logged. Records include information concerning normal re-calibration or synchronization of clocks used in time-stamping, as well as all events relating to detection of loss of synchronization.

c) Records concerning qualified time-stamping service are held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSA terms and conditions.

7.13. Business continuity management

Refer to clause 7.11 of [QTS PS].

Additionally, TSA Business continuity plan address the events of compromise or suspected compromise of TSU's private signing keys or loss of calibration of a TSU clock.

7.14. TSA termination and termination plans

Refer to clause 7.12 of [QTS PS].

Additionally:

a) TSU private keys are destroyed in a manner such that the private keys cannot be retrieved.

b) The TSA revokes all non-expired TSU's certificates.

7.15. Compliance

Refer to clause 7.13 of [QTS PS].

7.16. Supply chain

Refer to clause 7.14 of [QTS PS].

8. ADDITIONAL REQUIREMENTS FOR QUALIFIED ELECTRONIC TIME-STAMPS AS PER REGULATION (EU) No 910/2014

8.1. TSU public key certificate

A time stamp is declared by the MitSoft TSA to be a qualified electronic time stamp as per Regulation (EU) No 910/2014, and the TSU signature verification (public) key certificate was issued in compliance with the NCP+ certificate policy as specified in ETSI EN 319 411-1.

The time stamp issued by the MitSoft TSA contains non-critical qcStatements extension with a value esi4-qtstStatement-1 as defined in the Annex B of the ETSI EN 319 422.

8.2. TSU issuing non-qualified and qualified electronic time-stamps as per Regulation (EU) No 910/2014

MitSoft TSA issues time-stamps that are to be qualified electronic time-stamps as per Regulation (ES) No 910/2014.

MitSoft TSA issues time-stamps using two different TSU's issuing qualified electronic time-stamps to ensure high availability of the service.

MitSoft TSA issues qualified time-stamps and does not issue non-qualified electronic time-stamps.