mitsoft

Qualified Time-Stamping Service

Terms and Conditions

QTSS/TC

Version 1.01

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
1.01	2026-09-01	Updated list of legal acts and standards

Approval of the document

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

1. Purpose. The MitSoft time-stamping service provider (further – TSA) of the joint stock company "MIT-SOFT" (further – the MitSoft) discloses the general terms and conditions of the time-stamping service to the subscribers and relying parties. Qualified time-stamping service and qualified electronic time stamps provided by the MitSoft TSA 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, and the standards ETSI EN 319 421 "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" and ETSI EN 319 422 "Electronic Signatures and Infrastructures (ESI); Time-stamping Protocol and time-stamp token profiles". The terms and conditions stated here can be complemented by the Subscriber agreements between the TSA and the subscribers.

2. Contact information. All issues concerning the time-stamping 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

Qualified electronic time stamps can be obtained by accessing the service located at https://qtsp.mitsoft.lt/tsa. Requests of registered users are serviced using:

a) HTTPS protocol, if authenticated by username and password, according to the HTTP "basic" scheme;

b) HTTPS or HTTP protocol, if identified by IP address.

For user registration, the above contact information can be used.

3. Time-stamping service policy. Time-stamping service is provided according to the BTSP time-stamping policy (OID: 0.4.0.2023.1.1), defined in the standard ETSI EN 319 421.

The users of the time-stamping service provided by TSA can be legal or natural persons.

4. Hash of the data. The following algorithms can be used for computing a hash of the data to be time-stamped: SHA256, SHA384, SHA512, SHA3-256, SHA3-384, SHA3-512.

5. Certificate validity. TSA has 2 separate time-stamping units (TSUs). Each TSU uses one certificate, which is used to confirm the time stamp tokens issued by TSU. TSU's certificates are issued by the MitSoft TSA and used for time-stamping service only. The lifetime of the TSU's certificate is 7,5 years; TSU's private key usage period is 3 years; rekeying of the TSU's key (issuance of the new certificate) is performed every 2 years.

6. Accuracy of time stamp tokens. The value of time specified in a time stamp token denotes the time stamp generation moment with the accuracy of ***half of the second*** (or 500 ms). 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.

7. Limitations on the use. TSA does not set any limitations on the use of time-stamping service other than declared in this Terms and Conditions and Subscriber Agreement.

8. Subscriber obligations. Subscriber obligations are to accept time-stamping service terms and conditions and other duties stated in Subscriber agreement.

9. Relying party obligations. The relying party, when relying upon a qualified electronic time stamp, shall verify validity of time stamp received.

10. Verification of a time stamp token. If the time stamp token is verified during the TSU's certificate validity period, the validity of the signing key can be checked by making sure that the TSU's certificate has not been revoked. However, the qualified electronic time stamp can be verified even when the validity period of the certificate is expired provided that at the moment of verification it can be known that:

a) the TSU private key has not been compromised at any time up to the time of the qualified electronic time stamp verification;

b) the hash algorithms used in the time stamp token exhibit no collisions at the time of verification;

c) the signature algorithm and signature key size under which the time stamp token has been signed are still technologically reliable and beyond the reach of cryptographic attacks at the time of verification.

Information necessary to verify the qualified electronic time stamps is continuously available.

11. Information for parties relying on TSA Time-stamping service.

TSA obligation is to inform Subscribers and parties relying on the trust service of precise terms and conditions before entering into a contractual relationship. 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.

12. Service availability. MitSoft TSA time-stamping service is available 7 days a week and 24 hours per day.

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

14. Applicable law. TSA 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;
- 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;
- The standard ETSI EN 319 401: "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers";
- The standard ETSI EN 319 421 "Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps";
- The standard ETSI EN 319 422 "Electronic Signatures and Infrastructures (ESI); Time-stamping Protocol and time-stamp token profiles";

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

15. Settlement of disputes and complaints. All the complaints and disputes between TSA 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.

16. Liability, warranty and its limitations. TSA is liable for its illegal operation and reimburses the harm incurred by the subscriber as compelled by the law of the Republic of Lithuania. TSA undertakes no additional obligations, except for those determined in the Subscriber agreements for provision of service in effect.

17. Applicable agreements and practice statement. TSA provides the time-stamping service according to the time-stamping service policy (OID: 0.4.0.2023.1.1), following the Practice statement (OID: 1.3.6.1.4.1.57890.1.3.1), this Terms and Conditions document as well as the Subscriber agreements with subscribers.

18. Audit. The compliance of TSA's activities with the time-stamping service policy and the time-stamping service practice statement is verified in a way determined by the Practice statement.

19. Assessment of service conformance and assessment scheme. The TSA ensures compliance with the requirements of the Regulation (EU) No 910/2014 by an audit performed by an accredited conformity assessment body.

20. Service accessibility. TSA makes its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations.

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