BALTSTAMP TSA DISCLOSURE STATEMENT

1. Purpose. The BalTstamp time-stamping authority (further – TSA) of the joint stock company "BalTstamp" (further – the BalTstamp) discloses the general terms and conditions of the time-stamping services to the subscribers and relying parties. The time-stamps provided by the BalTstamp 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 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps" (previously published as ETSI TS 102 023 "Policy requirements for time-stamping authorities") and ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles" (previously published as ETSI TS 101 861 "Time stamping profile"). The terms and conditions stated here can be complemented by the contracts between the TSA and the subscribers.

2. Contact information. All issues concerning the time-stamp provision can be addressed to the contacts below:

Person:	Vincentas Vitkauskas, the director of the joint stock company "BalTstamp"
Address:	Dariaus ir Girėno st. 40, LT-02189 Vilnius
Phone:	+370-682-58844
Fax:	+370-5-2167212
URL:	http://www.baltstamp.lt/
E-mail:	info@baltstamp.lt

A time-stamp can be obtained by accessing the service located at http://tsa.baltstamp.lt using the standard RFC 3161 protocol. However, the limitation applies to non-registered users: no more than 100 requests within one month; the beginning and the end of the month are defined in UTC time. Requests of the registered users are serviced using:

a) a secure (https) protocol and identified by a username and password combination, according to the HTTP "basic" scheme;

b) an open (http) protocol and identified by IP address.

The flow of requests is limited to 5 requests per second and 1000 requests per hour unless otherwise is specified in the contract with the subscriber.

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

3. Time-stamp policy. All time-stamps are issued according to the best practices time-stamp policy (BTSP, OID: 0.4.0.2023.1.1), defined in the standard ETSI EN 319 421.

The time-stamp allows to prove that the electronic signature has been created before the time indicated in the time-stamp. However, it is possible to time-stamp unsigned data too. Such a time-stamp confirms that the data have been created before the time indicated in the time-stamp.

The users of the time-stamps provided by the TSA can be legal or natural persons needing the services provided by the TSA.

4. Hash of the data. The following algorithms can be used for computing a hash of the data to be time-stamped: SHA1, SHA256, SHA384, SHA512.

5. Certificate validity. TSA has two certificates used in the time-stamping units (TSUs) to confirm the time-stamp tokens issued. The lifetime of one certificate is 5 years; the validity expires on June 13, 2016. The lifetime of the other certificate is 10 years; the validity expires on May 15, 2022.

6. Precision of time-stamp tokens. The value of time specified in a time-stamp token denotes the time-stamp generation moment with the precision of ***two tenths of a second***, which is based upon permanent traceability of the TSA equipment to the State Standard of Time and Frequency realizing the Lithuanian universal coordinated time scale UTC(LT), which traceability to UTC is ensured by means of continuous comparison at the Time and Frequency Standard Laboratory of Metrology Department of the Center for Physical Sciences and Technology, which takes part in the generation of the universal coordinated time, as required by the standard ETSI EN 319 421. The characteristics of the traceability are published in the "Circular T" of the Bureau International des Poids et Mesures (BIPM).

7. Limitations on the use. TSA does not set any limitations on the use of its time stamps. They can be used when signing and carrying out electronic transactions, submitting applications and proposals, archiving electronic documents, etc.

8. Subscriber obligations. Having obtained a time-stamp token, the subscriber shall verify that the time-stamp token has been correctly signed, and the private key used has not been compromised.

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

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. But, if the time of verification is beyond the end of the validity period of the corresponding certificate, time-stamp verification may be impossible because certification authorities are not obliged to publish revocation data of expired certificates, including the revocation due to key compromise. However, the 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 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 time-stamps is constantly available.

11. Event logs. The journals of the TSA system operation and activity registration (event logs), which can be used as a legal evidence when necessary, are maintained for 10 years, and at least for 1 year after the expiration of the corresponding signing key.

12. Applicable law. TSA operates in the Republic of Lithuania and follows its 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;
- The standard ETSI EN 319 421 "Policy and Security Requirements for Trust Service Providers issuing Time-Stamps", previously published as ETSI TS 102 023 "Policy requirements for time-stamping authorities";
- The standard ETSI EN 319 422 "Time-stamping protocol and time-stamp token profiles", previously published as ETSI TS 101 861 "Time stamping profile".

13. Settlement of disputes and complaints. All the complaints and disputes between the 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.

14. 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 contracts for provision of service in effect.

15. Applicable agreements and practice statement. TSA provides the time-stamping services according to the Best practices time-stamp policy (OID: 0.4.0.2023.1.1), following the Practice statement (OID: 1.3.6.1.4.1.38424.1.4.1), the Disclosure statement as well as the contracts with subscribers.

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