

BALTSTAMP CERTIFICATION AUTHORITY

PKI Disclosure Statement

Version: 1.0

Valid since 2026-09-01

2026

Table of contents

1. Intruduction	3
2. TSP contact info.....	3
3. Certificate type, validation, procedures and usage	3
4. Reliance limits.....	4
5. Obligation of subject.....	4
6. Certificate status checking obligations of relying parties	5
7. Limited warranty and disclaimer/Limitation of liability:	5
8. Applicable agreements, CPPS	5
9. Privacy policy:.....	6
10. Refund policy:.....	6
11. Applicable law, complaints and dispute resolution:	6
12. TSP and repository licences, trus marks, and audit.....	7

The history of the BalTstamp Certificate Policy and Practice Statement:

Version	Valid since	Description
1.00	2026-09-01	The first official version of the document

Approval of the document

	Name	Date	Signature
Prepared by	Sandra Kočetkova	2026-06-04	
Verified by	Algirdas Ališauskas	2026-06-04	
Approved by	Sabina Sinicienė	2026-06-04	

1. Intruduction

This document contains the standard terms and conditions for the EU Electronic Seals (hereinafter referred to as the certificates)

These Terms and Conditions apply to BalTstamp in its capacity as the Trust Service Provider (TSP) and as the certificate holder. BalTstamp is responsible for the use and management of the certificate. The Terms and Conditions shall be deemed accepted upon issuance of the certificate.

*TSP is the Trusted Service Provider who is the issuer of the certificate and is the overall responsible entity for the certification services.

2.TSP contact info

TSP: UAB BalTstamp
Address: Dariaus ir Girėno g. 40, LT-02189 Vilnius
Telephone: +37 672 50927
e-mail: info@baltstamp.lt

3.Certificate type, validation, procedures and usage

3.1 Certificate type:

All certificates within the BalTstamp PKI hierarchy are issued as X.509 Version 3 certificates and include the extensions required for their intended roles (CA, OCSP Responder, and Time-Stamping Authority). The certificate profiles implement the certification path, key usage, basic constraints, authority information access, and revocation information mechanisms defined in RFC 5280. Based on the reviewed certificate profiles, the certificates conform to the ITU-T X.509 Version 3 digital certificate standard and are designed to operate within an RFC 5280-compliant public key infrastructure.

3.2 Validation procedures:

After certificate generation, the issued certificate is transferred to the Internal Auditor for independent verification. The auditor validates the certificate profile, verifies the certification path (Root CA → Issuing CA → End-Entity Certificate), confirms the certificate validity period, key parameters, certificate extensions, and compliance with the applicable certificate policy.

The auditor also verifies that the certificate has been issued from the approved Certificate Signing Request (CSR) by comparing the public key contained in the certificate with the public key contained in the original CSR. Matching public key hashes confirm that the certificate was issued for the intended key pair and has been generated correctly.

All verification activities and results are documented in a Certificate Validation Report.

Upon successful validation and approval by the National Communications Regulatory Authority (RRT), the certificate is transferred to the IT Administrator for deployment. The IT Administrator installs the certificate and corresponding trust chain on the production timestamping servers and makes the service available to relying parties.

Following deployment, the Security Manager updates the public repository with the current certificates, certification chain, revocation information, and related trust service documentation to ensure availability to customers and relying parties.

4. Reliance limits

4.1 Limitation of use:

The certificate is only to be used for PKI based services.

The key usage for the end-user certificates is set in the certificate profiles in the "Key Usage" field" and in the "Extended Key Usage" see "Appendix 1, OCSP Certificate Profiles" in the CPPS

The TSP is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations in its CPPS.

The intention or negligence of the TSP is presumed unless that the TSP proves that the damage occurred without the intention or negligence of the TSP. TSP is not liable for damages arising from the use of services exceeding the indicated limitations above and exceeding of the obligation of subscriber and subject indicated in "4. Obligation of subscriber and subject" below.

5. Obligation of subject

A subscriber is a legal person bound by agreement with a trust service provider to any subscriber obligations. The subscriber shall fulfil all obligations of the subscriber agreement. The subject shall fulfil all obligations of the subject agreement. If the subscriber and subject are separate entities, the subscriber shall make the subject aware of those obligations applicable to the subject.

The subscriber shall:

- a) Submit accurate and complete information to the TSP in accordance with the requirements in the certification practice statement.
- b) Maintain the correct information about the subscriber and subject, and notify the TSP of any changes to this information.
- c) Notify the TSP if any information in the Certificate is incorrect.
- d) Request the certificate to be revoked when a valid revocation reason exists (see "4.9.1 Circumstances for Revocation").
- e) In the case of being informed that the CA has been compromised, ensure that the private key is no longer used by the subject.
- f) Inform the TSP if an authorized subscriber representative no longer is authorized to represent the subscriber.
- g) Exercise reasonable care to avoid unauthorized use of the subjects' private keys.

Particularly keep the activation data (PIN) secret

- h) Ensure that restrictions on the subject's private key and the certificate are kept at all times.
- i) Ensure that the use of the subject private keys is immediately and permanently discontinued in case of private key compromise. For instance if control of the subject private keys are lost.
- j) Cease the use of the private keys at the end of the key usage periods (use for key decipherment is accepted).
- k) Ensure the key pair is only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person. Limitation is notified in each

certificate associated PDS (see also section "9.17 Other Provisions" under "Terms and Condition");

l) Use and maintain the subject's private key under the subject's control.

m) Notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate: i) the subject's private key has been lost, stolen, potentially compromised or; ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons.

n) Ensure that use of the certificate is under subscriber control by recording all entities that use and have access to the private keys, included processes, systems and individuals.

o) Private keys are generated within a cryptographic module and to use recommended cryptographic algorithm and parameters defined by ENISA.

The subject shall act according to the following points; a), d), e) g), h), i) , j), k) l) m) n) o)

(If the subscriber is the same entity as the subject, then all the subscriber obligations apply to the subject as well).

6.Certificate status checking obligations of relying parties

Relying parties are entitled to, when the certificate is used in a service, to check a certificate's status using the CRL and/ or the OCSP service related to that specific certificate to verify if a certificate is revoked and to see the status of the certificate being used. (The obligation to relying parties is described in more details in the CPPS).

7. Limited warranty and disclaimer/Limitation of liability:

See «3. Reliance limits:»

8. Applicable agreements, CPPS

The applicable CPPS is to be found here: <https://baltstamp.lt/en/documentation/>
Certificate Policy Identifier: (ETSI EN 319 411-1 [NCP+] 1.3.6.1.4.1.38424.1.2.X
The "X" implies digits for the latest versions.

9. Privacy policy:

The TSP is undertaking technical and organizational measures against unauthorized and unlawful processing of personal data and against accidental loss and destruction of, and damage to, personal data.

Records associated with a certificate (including information used under registration, subject device provision both from subscriber and subject, any subsequent revocation, the identity and any specific attributes placed in the certificate) are retained for (12) years following the date the Certificate expires or is revoked. These records may be passed to third parties under the same conditions as required by the existing CPPS in the case of the TSP terminating its services.

The following information/records are kept confidential and private (treated as private): CA application records, whether approved or disapproved; Certificate application records; Transactional records and the audit trail of transactions;

The following information/records will be made publicly available:

Certificates and their belonging public keys. Certificates and their belonging public key is publicly available at the TSP's LDAP service.

Certificate status. A certificate's status is publicly available at the TSP's CRL and OCSP service.

When the TSP intends to make changes to its PKI Disclosure Statements (PDS) and the associated CPPS that might affect the acceptance of the service by the subject, subscriber, or relying parties, it will publish the changes with details at <https://www.baltstamp.lt/Documents> under the heading "Previous versions and change log."

10. Refund policy:

N/A

11. Applicable law, complaints and dispute resolution:

BalTstamp UAB shall maintain documented procedures for the receipt, registration, investigation, resolution, and retention of records relating to complaints and disputes associated with its certification services.

Complaints may be submitted by relying parties, supervisory authorities, auditors, business partners, or other affected parties regarding the operation of the Certification Authority (CA), certificate status services, repository services, or other certification activities.

The complainant shall provide sufficient information to enable investigation, including:

- Identification of the affected certificate(s), service, or transaction;
- Description of the incident or disputed matter;
- Date and time of the incident, where applicable;
- Any supporting information or evidence relevant to the complaint.

Complaints shall be submitted using the contact information published in the Certification Authority's public repository.

Upon receipt of a complaint, BalTstamp UAB shall:

- Acknowledge receipt of the complaint;
- Register the complaint in the complaint and incident management system;
- Investigate the matter and assess any impact on certification services;
- Document findings, decisions, and corrective actions, where applicable;
- Communicate the outcome of the investigation to the complainant within a reasonable period.

11.1 Dispute Resolution

BalTstamp UAB shall seek to resolve disputes through consultation and good-faith negotiations whenever possible. Where a dispute cannot be resolved amicably, the matter shall be referred to the competent courts of the Republic of Lithuania.

11.2 Governing Law

The operation of the Certification Authority, the provision of certification services, and any related disputes shall be governed by:

- The laws of the Republic of Lithuania;
- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions (eIDAS), and subsequent applicable European Union legislation;
- Applicable Lithuanian legislation governing trust services, electronic signatures, electronic seals, and public key infrastructure services.

12.TSP and repository licences, trus marks, and audit

BalTstamp UAB is a Qualified Trust Service Provider (QTSP) as defined in Regulation (EU) No 910/2014 (eIDAS) and provides qualified trust services under the supervision of the Communications Regulatory Authority of the Republic of Lithuania (RRT).

BalTstamp UAB is CA (Certificate Authority) for Qualified Certificates for electronic seals.

BalTstamp UAB is a Qualified Trust Service Provider (QTSP) supervised by the Communications Regulatory Authority of the Republic of Lithuania (RRT). BalTstamp fulfils and operates in accordance with ETSI EN 319 401, ETSI EN 319 411-1 and other applicable ETSI standards. BalTstamp is subject to periodic conformity assessments by an accredited conformity assessment body, and the resulting conformity assessment reports are submitted to RRT. Qualified trust services provided by Baltstamp are published in the Lithuanian Trusted List maintained by RRT and are included in the European Union Trusted List system in accordance with Regulation (EU) No 910/2014 (eIDAS).