

BALTSTAMP CERTIFICATION AUTHORITY

Certificate Policy and Practice Statement

Unique object ID (OID): **1.3.6.1.4.1.38424.1.2.1**

Version: 1.0

Valid since 2026-09-01

Table of contents

1. INTRODUCTION	6
1.1. Overview.....	6
1.2. Identification	6
1.3. PKI participants	7
1.3.1. Certification authorities	7
1.3.2. Registration authorities	7
1.3.3. Subscribers.....	7
1.3.4. Relying parties.....	7
1.3.5. Other participants	7
1.4. Certificate usage.....	8
1.5. Policy administration	8
1.5.1 Organization administering the document.....	8
1.5.4 PPPS approval procedures	8
1.6. Definitions and abbreviations.....	9
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	10
3. IDENTIFICATION AND AUTHENTICATION	10
3.1 Naming.....	10
3.1.1 Types of Names	10
3.1.2 Need for Names to be Meaningful	11
3.1.3 Anonymity or Pseudonymity of Subscribers	11
3.1.4 Rules for Interpreting Various Name Forms	11
3.1.5 Uniqueness of Names	11
3.1.6 Recognition, Authentication, and Role of Trademarks	11
3.2 Initial Identity Validation.....	11
3.2.1 Method to Prove Possession of Private Key	11
3.2.2 Authentication of Organization Identity	11
3.2.3 Authentication of Individual Identity	11
3.2.4 Non-Verified Subscriber Information	12
3.2.5 Validation of Authority	12
3.2.6 Criteria for Interoperation.....	12
3.3 Identification and Authentication for Re-Key Requests	12
3.3.1 Identification and Authentication for Routine Re-Key	12
3.3.2 Identification and Authentication for Re-Key after Revocation	12
3.4 Identification and Authentication for Revocation Request.....	12
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	13
4.1. Certificate application.....	13
4.1.1 Who can Submit a Certificate Application.....	13
4.1.2 Enrollment Process and Responsibilities	13
4.2. Certificate application processing.....	13
4.3. Certificate issuance.....	13
4.4. Certificate acceptance	13
4.5. Key pair and certificate usage.....	13
4.6. Certificate renewal.....	13
4.7. Certificate re-key	14
4.7.1. Circumstance for certificate re-key	14
4.7.2. Who may request certification of a new public key.....	14
4.7.3. Processing certificate re-keying requests.....	14
4.7.4. Notification of new certificate issuance to subscriber.....	14
4.7.5. Conduct constituting acceptance of a re-keyed certificate.....	14
4.7.6. Publication of the re-keyed certificate by the CA.....	14
4.7.7. Notification of certificate issuance by the CA to other entities.....	14
4.8. Certificate modification.....	14
4.9. Certificate revocation and suspension.....	14
4.10. Certificate status services	15
4.11. End of subscription	15

4.12.Key escrow and recovery	15
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	15
5.1. Physical controls	15
5.2. Procedural controls	15
5.3. Personnel controls	15
5.4. Audit logging procedures	15
5.4.1 Types of events recorded	15
5.4.2 Frequency of processing log	16
5.4.3 Retention period for audit log	16
5.4.4 Protection of audit log	16
5.4.5 Audit log backup procedures	16
5.4.6 Audit collection system (internal vs. external)	16
5.4.7 Notification to event-causing Subject	16
5.4.8 Vulnerability assessments	16
5.5. Archiving the records	17
5.5.1 Types of records archived	17
5.5.2 Retention period for archive	17
5.5.3 Protection of archives	17
5.5.4 Archive backup procedures	17
5.5.5 Requirements for time-stamping of records	17
5.5.6 Archive collection system	17
5.5.7 Procedures to obtain and verify archive information	17
5.6. Key changeover	18
5.7. Compromise and disaster recovery	18
5.8. CA termination	18
6. TECHNICAL SECURITY CONTROLS	19
6.1. Key pair generation and installation	19
6.2. Private Key Protection and Engineering Controls of the	19
6.3. Other aspects of key pair management	19
6.3.1 Public Key Archival	19
6.3.2 Certificate Operational Periods and Key Pair Usage Periods	19
6.4. Activation data	20
6.5. Computer security controls	20
6.6. Life cycle technical controls	20
7. CERTIFICATE, CRL, AND OCSP PROFILES	21
7.1. Certificate Profiles	21
7.1.1. Root CA Certificate Profile	21
7.1.2. Issuing CA Certificate Profile	22
7.1.3. TSU Certificate Profile — TSU3	23
7.1.4. TSU Certificate Profile — TSU4	25
7.2. CRL Profiles	27
7.3. OCSP Responder Certificate profile	29
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	30
8.1 Frequency or Circumstances of Assessment	30
8.2 Identity/Qualifications of Assessor	30
8.3 Assessor's Relationship to Assessed Entity	30
8.4 Topics Covered by Assessment	30
8.5 Actions Taken as a Result of Deficiency	30
8.6 Communication of Results	30
9. OTHER BUSINESS AND LEGAL MATTERS	31
9.1 Fees	31
9.2 Financial Responsibility	31
9.3 Confidentiality of Business Information	31
9.4 Privacy of Personal Information	31
9.5 Intellectual Property Rights	31
9.6 Representations and Warranties	31
9.7 Disclaimers of Warranties	31
9.8 Limitations of Liability	31
9.9 Indemnities	31
9.10 Term and TerminationLimitations of Liability	31

9.11 Individual Notices and Communications with Participants..... 31

9.12 Amendments..... 31

9.12.1 Procedure for Amendment 31

9.12.2 Procedure for Amendment Notification Mechanism and Period..... 32

9.12.3 Circumstances Under Which OID Must be Changed 32

9.13 Dispute Resolution Provisions..... 32

9.14 Governing Law..... 32

9.15 Compliance with Applicable Law 32

9.16 Miscellaneous Provisions..... 32

9.17 Other Provisions..... 32

10. REFERENCES 34

The history of the BaITstamp 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	Emilis Urba	2026-06-01	
Verified by	Sandra Kočetkova	2026-06-01	
Approved by	Sabina Sinicienė	2026-06-01	

1. INTRODUCTION

Joint Stock Company BalTstamp (hereinafter referred to as "BalTstamp") was established on 31 January 2011 with the purpose of providing qualified time-stamping services to both legal and natural persons. These services are intended to support the long-term validity of qualified electronic signatures throughout the entire retention period of electronic documents containing such signatures.

Further information about BalTstamp is available on its website: <https://www.baltstamp.lt/>.

1.1. Overview

The BalTstamp Time-Stamping Authority (TSA) is responsible for issuing qualified electronic time stamps as well as the certificates used by the BalTstamp Qualified Time-Stamping Service (QTSS).

The BalTstamp CA Certificate Policy establishes the primary requirements governing certificates issued by the BalTstamp TSA, while the BalTstamp TSA Certification Practice Statement describes the practices and procedures implemented to satisfy those requirements. For ease of reference, these documents are combined into a single document, the BalTstamp CA Certificate Policy and Practice Statement (CPPS).

As the BalTstamp TSA issues certificates exclusively for the purposes of the QTSS, this CPPS document refers to relevant sections of the [BalTstamp TSPS] where appropriate, thereby avoiding duplication of requirements.

This CPPS has been developed in accordance with the requirements of ETSI EN 319 411-1 [EN 319 411-1], adapted as necessary to meet the specific needs of the QTSS.

Terminology

Unless otherwise specified in this document:

- **Time stamps** refers to qualified electronic time stamps as defined in Regulation (EU) No. 910/2014 [eIDAS].
- **Certificate Policy** refers to the BalTstamp TSA Certificate Policy.
- **Certification Practice Statement** refers to the BalTstamp TSA Certification Practice Statement.
- **BalTstamp TSA** and **BalTstamp QTSA** refer to the BalTstamp Time-Stamping Authority.

1.2. Identification

The BalTstamp CA Certificate Policy and Practice Statement is identified by the following object identifier (OID): **1.3.6.1.4.1.38424.1.2.1**. The values associated with its fields are presented in Table 1.

Table 1. Field Values of the BalTstamp CPPS Object Identifier (OID)

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 "BalTstamp"	38424
Subdivision: Qualified trust services	1
Document type: BalTstamp CA Certificate Policy	2
Document version	1

1.3. PKI participants

The BalTstamp Certification Authority (CA) is operated exclusively for the issuance of certificates required by the BalTstamp Qualified Time-Stamping Service (QTSS). The CA is not intended for, and shall not be used in, any other application or service.

As certificates are issued solely for internal QTSS purposes, no Registration Authority (RA) is established or operated.

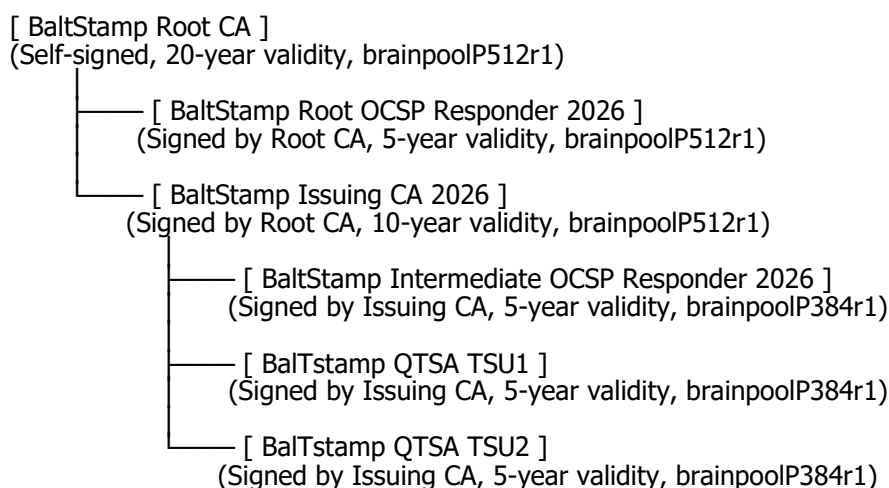
The TSA issues certificates exclusively for the internal needs of the BalTstamp Qualified Time-Stamping Service and, consequently, does not maintain or serve external subscribers.

1.3.1. Certification authorities

Two certificate hierarchies with identical structures are maintained. The cryptographic keys and certificates associated with each hierarchy are stored and managed within separate dedicated Hardware Security Modules (HSMs).

At the top of each hierarchy is a self-signed Root Certification Authority (Root CA) certificate. The Root CA is used to issue certificates to Time-Stamping Units (TSUs) and to sign Certificate Revocation Lists (CRLs).

Certificate hierarchies of TSA are presented in the following picture:



BalTstamp TSA generates and stores the private keys associated with the self-signed Root CA certificates and TSU certificates within dedicated Hardware Security Modules (HSMs) certified as Qualified Signature Creation Devices and Qualified Seal Creation Devices (QSCDs) under the eIDAS framework.

The HSMs used by BalTstamp TSA are secure cryptographic devices that provide an assurance level of EAL4+ or higher in accordance with ISO/IEC 15408 [ISO 15408].

1.3.2. Registration authorities

The Registration Authority is operated solely by BalTstamp for its own purposes.

1.3.3. Subscribers

Not applicable.

1.3.4. Relying parties

TSA certificates are intended to be used by relying parties of the BalTstamp Qualified Time-Stamping Service (QTSS) for the validation of qualified electronic time stamps.

1.3.5. Other participants

Policies and Procedures Management Body (PPMB) is a committee created in BalTstamp in order to supervise the entire activity of all trust services. The responsibilities of PPMB consist of:

- Reviewing and approving the CPPS

1.4. Certificate usage

Refer to clause "4.5 Key pair and certificate usage".

1.5. Policy administration

BalTstamp TSA Certificate Policy is managed by the joint stock company "BalTstamp", which contact information is given in the BalTstamp TSA Disclosure Statement in effect, which is available at the website <https://www.baltstamp.lt/>.

The director of the BalTstamp TSA has overall responsibility for the CA with final authority for approving the CPPS.

1.5.1 Organization administering the document

The present document is administered by the BalTstamp Trust Service Provider (TSP) through the Policies and Procedures Management Body (PPMB). The PPMB includes senior members of the management as well as staff responsible for the operational management of the BalTstamp TSP environment.

1.5.4 PPPS approval procedures

Policies and Procedures Management Body is responsible for the approval of the PPPS. Subscribers shall adhere to the PPPS implemented and published at:

<https://www.baltstamp.lt/>.

1.6. 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 [1].

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: 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.

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-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 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 [EN 319 401].

CA Certification Authority

CP Certificate Policy

CRL Certificate Revocation List

CPPS BalTstamp TSA Certificate Policy and Practice Statement

ESI Electronic Signature and Infrastructure

ETSI European Telecommunications Standards Institute

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)

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

All certificates and Certificate Revocation Lists (CRLs) are published in the BalTstamp repository. The repository is publicly accessible to subscribers and relying parties.

TSU certificates are made available in the repository only after their inclusion in the Trusted List of Lithuania.

CRLs are also publicly accessible via the BalTstamp repository.

Regular CRLs are published at least every 24 hours. An additional (irregular) CRL may be issued and published immediately following the revocation of a certificate.

BalTstamp publishes and maintains both the CPPS (Certificate Policy and Practice Statement) and the PDS (PKI Disclosure Statement).

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The CA certificates contain X.501 distinguished names in the issuer and subject fields. Issuer distinguished names consist of the components specified in the table below.

Attribute	Value
Country (C)	The CAs country or origin.
Organization (O)	Indicates the controlling organization of the CA
Organizational Unit (OU)	The CA certificates contain several OU attributes which specify the CA's position in the CTE hierarchy and type of certificate issued.
State or Province (S)	Indicates the CAs state or province.
Locality (L)	Indicates the CAs city.
Common Name (CN)	This attribute is the common name of the CA.

Attribute	Value
Country (C)	Indicates the subscriber's Country.
Organization (O)	Subscriber's organizational or company name for Subscriber's personal certificate or not used.
Organizational Unit (OU)	The subscriber certificates may contain multiple OU attributes. Such attributes may contain one or more of the following: subscriber organizational unit. An indication of which CA issued the Certificates. "Authenticated by BalTstamp" or other entity in certificates whose applications were authenticated by BalTstamp or other entity.
Organization Identifier	NTRNO-<Business number as stated in Registry Centras or other applicable identification practices>
State or Province (S)	Indicates the subscriber's state or province or not used.
Locality (L)	Indicates the subscriber's locality or not used.

Common Name (CN)*	This attribute includes the name of the individual or device (hostname in the case of server Certificates).
-------------------	---

The subscriber certificates contain an X.501 distinguished name in the subject name field and consist of the components specified in Table below.

*Common Name (CN)

- Component of the subject distinguished name of subscriber certificates is authenticated.
- Subject name e.g. subscriber name, system name, application name, or domain name owned by the company can be included.

3.1.2 Need for Names to be Meaningful

CA Certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the subject of the certificate.

For use of email address, the address must be meaningful

For subscriber certificates the full name and legal status of the subscriber as defined in the national business register or equivalent for Legal Entities must be used and it must be able to identify both certificate applicants and subject sponsors as authorized subscriber representatives.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymity or Pseudonymity of subscribers is not allowed.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

All CA certificates names are unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

For role of Trademark see CPPS section "9.5 Intellectual Property Rights".

3.2 Initial Identity Validation

BalTstamp Certification Authority (CA) issues certificates exclusively for the internal operation of the BalTstamp Qualified Time-Stamping Service (QTSS). The CA does not provide certification services to external subscribers. Certificate issuance is performed only through internal procedures by trusted personnel under dual control.

3.2.1 Method to Prove Possession of Private Key

Not applicable. Key pairs are generated and controlled by BalTstamp within HSMs.

3.2.2 Authentication of Organization Identity

Not applicable.

3.2.3 Authentication of Individual Identity

Not applicable.

3.2.4 Non-Verified Subscriber Information

Not applicable.

3.2.5 Validation of Authority

Not applicable. Certificate issuance is performed only through internal procedures by trusted personnel under dual control.

3.2.6 Criteria for Interoperation

Not applicable.

3.3 Identification and Authentication for Re-Key Requests

The TSP doesn't offer certificate re-key.

3.3.1 Identification and Authentication for Routine Re-Key

The TSP doesn't offer certificate re-key.

3.3.2 Identification and Authentication for Re-Key after Revocation

The TSP doesn't offer certificate re-key.

3.4 Identification and Authentication for Revocation Request

Revocation of TSU certificates is performed in accordance with Section 4.9 "Certificate Revocation and Suspension" of the BalTstamp Certificate Policy and Practice Statement.

As BalTstamp TSA issues certificates exclusively for the internal operation of the BalTstamp Qualified Time-Stamping Service (QTSS), no external subscribers are permitted and no subscriber-initiated certificate revocation requests are accepted.

A TSU certificate revocation may be initiated only by authorized BalTstamp personnel in accordance with internal procedures and upon a decision of BalTstamp management. Circumstances that may result in certificate revocation include, but are not limited to:

- Loss, compromise, or suspected compromise of a TSU private key;
- An official request from a law enforcement authority; or
- Other security or operational events requiring certificate revocation.

The circumstances surrounding a potential revocation event shall be investigated before a revocation decision is made. Once the revocation decision has been approved, authorized TSA personnel shall perform the revocation using documented internal procedures.

Information concerning revoked certificates shall be published through the BalTstamp repository and associated Certificate Revocation Lists (CRLs). Where applicable, BalTstamp shall also notify the Communications Regulatory Authority of the Republic of Lithuania (RRT) and other relevant relying parties in accordance with established procedures.

Certificate suspension is not supported.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Certificates are issued to the BalTstamp Qualified Time-stamping Service using internal procedures implementing the requirements for TSU key generation as defined in ETSI EN 319 421 [EN 319 421].

4.1. Certificate application

4.1.1 Who can Submit a Certificate Application

BalTstamp CA issues certificates exclusively for the purposes of the QTSS,

4.1.2 Enrollment Process and Responsibilities

All certification processes are performed under the TSP control by trusted personnel in trusted roles

4.2. Certificate application processing

Not applicable.

4.3. Certificate issuance

TSU certificates are issued to BalTstamp Qualified Time-Stamping Service only. Other subscribers are not allowed to submit certificate applications.

Key generation for self-signed root CA certificates and TSU certificates and the certificates issuance is performed only by personnel in trusted roles under at least dual control ensured by internal procedures.

4.4. Certificate acceptance

Not applicable.

4.5. Key pair and certificate usage

BalTStamp Root CA: This is a self-signed certificate that serves as the trust anchor for the entire PKI. Its primary usage is to sign and issue certificates for the next level of the hierarchy, specifically the Intermediate CA and the Root OCSP Responder. It is also used to generate the Certificate Revocation List (CRL) for the root level. Any other use of the Root CA private keys is not permitted.

BalTStamp Issuing CA 2026 (Intermediate CA): Signed by the Root CA, this certificate acts as the operational issuing authority. Its purpose is to sign and issue end-entity certificates, including the TSU certificates and the Intermediate OCSP Responder. It also manages revocation for its tier by generating a regular CRL. Any other use of the Issuing CA private keys is not permitted.

TSU private keys shall be used only for signing time-stamps generated by the BalTstamp Qualified Time-Stamping Service. Any other use of TSU private keys is strictly prohibited.

Private keys shall not be used beyond their defined key usage period.

Relying parties shall use TSU certificates and public keys exclusively for the purposes of time-stamp validation and TSU identification.

4.6. Certificate renewal

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

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

QTSS shall use valid TSU certificates with a non-expired private key usage period, therefore, BalTstamp TSA ensures regular and timely TSU certificate re-key. In addition to regular TSU certificate re-key, TSU certificate re-key is performed if:

- data placed in the TSU certificate does not correspond to the legal status of TSA;
- cryptographic algorithms used for time stamp creation are changed, due to BalTstamp QTSP business decision;
- TSU certificate profile was modified, due to its non-compliance with the requirements of the updated standards, legal acts or due to BalTstamp TSA business decision;
- certificate revocation occurs.

Root CA certificate re-key is performed only because of its expiration or loss of the corresponding key.

4.7.2. Who may request certification of a new public key

Certificate re-key is performed at a request by the BalTstamp TSA only.

4.7.3. Processing certificate re-keying requests

Not applicable.

4.7.4. Notification of new certificate issuance to subscriber

Not applicable.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6. Publication of the re-keyed certificate by the CA

Newly issued certificates are published in the BalTstamp repository.

4.7.7. Notification of certificate issuance by the CA to other entities

BalTstamp TSA informs Communications Regulatory Authority of the Republic of Lithuania (RRT) performing role of National Supervisory Body of qualified trust service providers about new TSU certificate issuance for BalTstamp QTSS. BalTstamp TSA asks RRT to initiate the procedure for including a new TSU certificate in the Trusted list of Lithuania.

4.8. Certificate modification

Certificate modification, defined as the issuance of a new certificate with updated attributes while retaining the same public key, is not supported. Instead, certificate re-keying, involving the issuance of a new certificate with a newly generated public key, is performed.

4.9. Certificate revocation and suspension

TSU certificate revocation can be triggered by unexpected events such as loss of the TSU 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 BalTstamp.

Revocation is performed by the TSA personnel using internal procedures.

The information about revoked certificate is announced on the BalTstamp website.

The subscribers of the BalTstamp Qualified Time-Stamping Service are also informed via contact information provided to TSA by the subscribers.

Additionally, TSA informs Communications Regulatory Authority of the Republic of Lithuania (RRT) performing role of National Supervisory Body of qualified trust service providers about TSU

certificate revocation. RRT may use its own procedures to inform other relying parties about TSU certificate revocation. TSU certificate suspension is not applicable.

4.10. Certificate status services

BalTstamp TSA provides Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) services for certificate status checking.

Regular CRLs are published at least every 24 hours and are made publicly available through the BalTstamp repository. Additional CRLs may be issued and published immediately following the revocation of a certificate.

The OCSP service provides real-time certificate status information and is publicly available to relying parties and other authorized users. OCSP responses are signed by a dedicated OCSP Responder certificate issued by the BalTstamp Certification Authority.

Issued CRL fields are described in Section 7.2 "CRL Profiles", while OCSP response profiles and related service information are described in Section 7.3 "OCSP Profiles".

4.11. End of subscription

Not applicable.

4.12. Key escrow and recovery

The TSP doesn't offer key escrow of private keys for end-user certificates.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

BalTstamp TSA uses the same physical and environmental security facilities, procedural and personal controls as for Qualified Time Stamping Service operation and management.

5.1. Physical controls

Refer to clause 3.8 of [BalTstamp TSPS].

5.2. Procedural controls

Refer to clause 3.3 of [BalTstamp TSPS].

5.3. Personnel controls

Refer to clause 3.3 of [BalTstamp TSPS].

5.4. Audit logging procedures

5.4.1 Types of events recorded

For all events related to the CA key operations, records will be kept that include all information related to that event that can be useful for auditing purposes.

Extensive security logging and monitoring is performed at various levels including (non-exhaustive):

- the physical level (including equipment cabinet access)
- the network level
- the operating system level
- the application level

The PKI software and associated routines may record events that include but are not limited to:

- Issuance of a certificate: request, approval or rejection (with reason) of request, registration information,

Identification of the RA approving or processing the request, certificate generation/activation.

- Revocation of a certificate: revocation request, approval or rejection (with reason) of request, Identification of the RA approving or processing the request, Identification of the requestor.
- Publishing of a CRL

The audit logs records contain:

- The identification of the operation.
- The date and time of the operation.
- The identification of the certificate, if applicable.
- The identity of the transaction.

In addition, audit logs of relevant operational events in the infrastructure are maintained, including, but not limited to:

- Log in and log out of PKI components administrative interfaces.
- Start and stop of servers.
- Outages and major problems.
- Physical access of personnel and other persons to sensitive parts of the PKI site.
- Backup and restore.
- Report of disaster recovery tests.
- Audit inspections.
- Upgrades and changes to systems, software and infrastructure.
- Security intrusions and attempts at intrusion.

5.4.2 Frequency of processing log

The PKI operations staffs regularly monitor security related events. Information about critical events is forwarded to the appropriate department for immediate attention. Reports that are generated from the audit logs are reviewed by internal auditors.

5.4.3 Retention period for audit log

System logs are retained for 18 months. For audit logs for the CA and PKI components, see section 5.5.2.

5.4.4 Protection of audit log

The audit logs of the CA application software and PKI components application software are time stamped. CA audit logs are signed. The signature key is protected by an HSM. Consolidated logs are kept on secure storage systems or media and located or stored in a secure location.

5.4.5 Audit log backup procedures

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by PKI CA Officers. For key ceremonies, a relevant extract of the audit log is made and stored separately.

5.4.6 Audit collection system (internal vs. external)

The PKI audit collection system is internal.

5.4.7 Notification to event-causing Subject

Not applicable.

5.4.8 Vulnerability assessments

The entire infrastructure is subject of a vulnerability assessment and penetration testing at least once a year and ad-hoc if a critical part of the infrastructure is affected. The assessment covers the

ICT infrastructure, the special cryptographic equipment, the physical environment, data storage, software, personnel, processes and procedures and communication.

Vulnerability assessment of the audit log is part of the risk assessment and risk management program documented internally.

5.5. Archiving the records

5.5.1 Types of records archived

See section 5.4.1 and 5.5.2.

5.5.2 Retention period for archive

The archive retention periods for the various types of records are:

- issued certificates for a period of 7 years after the certificate ceases to be valid,
- audit trails on the issuance of certificates for a period of minimum 7 years after the certificate ceases to be valid,
- copies of identification documents are retained 7 years after any certificate based on these records ceases to be valid,
- audit trail of the revocation of a certificate for a period of minimum 7 years after revocation of the certificate,
- CRLs for at least 7 years after creation of the CRL,
- documentation supporting the issuance and use of the certificate is kept for a period of at least 12 years after the expiration of the last certificate supported by the documentation.

5.5.3 Protection of archives

The archives are protected against manipulation or willful destruction. As far as possible archive will be retained and protected in electronic form.

Paper-based records are archived and under control of the respective roles that process them. Paper-based archive may be stored on multiple locations according the requirements laid down in the applicable Policy document. Registration information will be securely stored to provide reasonable assurance regarding secrecy, integrity and availability.

5.5.4 Archive backup procedures

Backup copies of the relevant electronic system logs and electronic audit logs are stored in multiple locations.

5.5.5 Requirements for time-stamping of records

The date and time source for audit logs created by the core Trust Service components are synchronised with UTC using dedicated NTP equipment.

The TSP PKI operator operates Stratum-1 multi-GNSS referenced NTP infrastructure to synchronize the system clocks of critical infrastructure with external time references from the public NTP services of the UTC(LT).

5.5.6 Archive collection system

The archive collection system for the Trust Service components is internal infrastructure of the TSP PKI operator.

5.5.7 Procedures to obtain and verify archive information

The contents of the archive are not accessible except for authorized personnel of the TSP and with exception of obligations by law or by court order.

Access to an archive by authorized personnel must be motivated (e.g. in case of incident investigation, to test the "retrieval" procedure, etc.).

Disclosure of information from the archive upon request by an implicated party other than the Certificate Subject: the

TSP requires approval by the Management Body. The TSP reserves the right to charge a compensation to cover the expenses of the retrieval of the information from the archives.

5.6. Key changeover

The TSP CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in Section "6.3.2 Certificate Operational Periods and Key Pair Usage Periods". The TSP's CA certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services in accordance with Section "6.1 Key Pair Generation and Installation"

5.7. Compromise and disaster recovery

Refer to clauses 3.13 of [BalTstamp TSPS].

5.8. CA termination

Before a BalTstamp ceases its activity, the TSP will:

- Inform (at least 30 days in advance) the following about the decision to terminate its services: all Subscribers who hold active (unexpired and not terminated) agreements signed with BalTstamp and other entities with which BalTstamp has agreements or other form of established relations, among which relying parties, other trust service providers and relevant authorities such as supervisory bodies. In addition, this information will be made available to other relying parties;
- Transfer its obligations to a reliable party for maintaining all information necessary for the operation of the TSP services for a reasonable period.
- Where possible, make arrangements to transfer provision of TSP services for the existing customers to another trusted service provider.

BalTstamp will maintain or transfer to a reliable party its obligations to make available its TSP services for a reasonable period.

In case BalTstamp will terminate its activities without a partially or full transfer of its activities, will initiate the termination procedure for the contracts signed with the implied partners and/or suppliers.

BalTstamp has an arrangement to cover the costs to fulfil these minimum requirements in case it becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

Takeover by the successor of the terminated TSP

In order to ensure the continuity of TSP services for Subscribers, the terminating TSP may sign a contract with another TSP offering similar services to take over, under pre- determined conditions, the specific data and activities.

By taking over the activities, the successor to the TSP that ceases activity takes over the rights and obligations of this authority with regard to the management of the trusted services.

After notification of termination of the services by the BalTstamp TSP, the Subscriber has the decision whether to accept the continuation of the services with the new TSP or to withdraw from the agreement with BalTstamp.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

Key pair and certificate generation are performed only by trusted roles under, at least, dual control and are defined by the internal BalTstamp TSA procedures.

Private keys are generated within a cryptographic module, and never exported from it, and never imported into it.

Key lengths and cryptographic algorithms for CA and TSU signing keys are selected according recommendations in ETSI TS 119 312 [TS 119 312] in compliance with the Agreed Cryptographic Mechanisms endorsed by the European Cybersecurity Certification Group and published by ENISA for the CA's signing purposes.

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 7.1. Certificate profiles).

6.2. Private Key Protection and Engineering Controls of the Cryptographic Module

Private signing keys are held and used within a cryptographic module, which assure EAL4+ level or higher in accordance with ISO/IEC 15408 [ISO 15408].

The same key protection requirements are applied for the private keys of the root CA certificates as for the private keys of the TSU certificates defined in the clause 3.6.3 of [BalTstamp TSPS].

6.3. Other aspects of key pair management

6.3.1 Public Key Archival

The TSP CA and end-user subscriber certificates are backed up and archived as part of the TSP routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The operational period of a certificate ends upon its expiration or revocation. The operational period for key pairs is the same as the operational period for the associated certificates, all use of the key pair shall cease after their usage period have expired, except private keys may continue to be used for decryption and public keys may continue to be used for signature verification.

Certificates issued by CAs to end-user subscribers may have operational periods as specified in section 7.1. Certificate profiles

The root and its subordinate CA certificates all expires as specified in section 7.1. Certificate profiles

End-user certificates shall have an expiration date before their signing subordinate certificate.

6.4. Activation data

Certificate generation:

- The installation and recovery of the CA's key pairs in a secure cryptographic device require simultaneous control of at least two trusted employees.

Subject device provision:

- Secure cryptographic device (including smartcard) deactivation and reactivation are done securely.
- Where the secure cryptographic device (including smartcard) has associated user activation data (like PIN code), the activation data is securely prepared and distributed separately from the secure cryptographic device. Separation is allowed to be achieved by ensuring distribution of activation data and delivery of secure user device at different times, or via a different channel. See also CPPS section "4.3 Certificate Issuance".

6.4.1 Activation Data Generation and Installation

The TSP CA Private Key generation is carried out according to the TSP Key Ceremony by trusted personnel in trusted roles. The CA private key is randomly generated and stored using a secure encryption device.

6.4.2 Activation Data Protection

The TSP CA private key activation data is protected in a physically secured environment under dual control with at least two trusted personnel in trusted roles (see section "5.2.1 Trusted Roles")

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5. Computer security controls

Refer to clauses 3.5 of [BalTstamp TSPS].

6.6. Life cycle technical controls

Refer to clauses 3.6 of [BalTstamp TSPS].

7.CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profiles

The following subsections present the certificate profiles for each entity in the BalTstamp TSA certificate hierarchy. Each profile table contains both the normative requirements defined in the BalTstamp CPPS and the actual values from the certificates.

7.1.1. Root CA Certificate Profile

The self-signed Root CA certificate serves as the trust anchor for the entire BalTstamp PKI hierarchy. It is used exclusively to issue certificates to the Issuing CA, OCSP Responder, and to sign Certificate Revocation Lists. The certificate conforms to RFC 5280 and ETSI EN 319 412-3.

7.1.1.1 Certificate Fields

Table 1. Certificate fields — BalTstamp Root CA 2026

Field	Required	Description	Value (from BalTstamp Root CA 2026)
Version	Yes	X.509 version of the encoded certificate	Version 3 (0x2)
Serial Number	Yes	Positive integer assigned by the TSA	3e:12:d3:00:b2:c2:bc:7e:9b:2c: 9b:f7:3a:cb:fa:e5:3a:8e:da:68
Issuer DN	Yes	Entity that signed and issued the certificate	C = LT O = Baltstamp UAB CN = BalTstamp Root CA 2026 organizationIdentifier = NTRLT-302608545
Subject DN	Yes	Entity associated with the public key (self-signed)	C = LT O = Baltstamp UAB CN = BalTstamp Root CA 2026 organizationIdentifier = NTRLT-302608545
Not Before	Yes	Start of the certificate validity period	Jun 3 10:53:52 2026 GMT
Not After	Yes	End of the certificate validity period	May 29 10:53:52 2046 GMT (20 years)
Signature Algorithm	Yes	Algorithm used to sign the certificate	ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Subject Public Key Algorithm	Yes	Public key algorithm identifier	id-ecPublicKey (OID: 1.2.840.10045.2.1)
Elliptic Curve	Yes	Named elliptic curve used for the public key	brainpoolP512r1 (512-bit)
Public Key (partial)	Yes	Subject public key value	04:33:1f:b2:6f:2f:9d:5b:fb:c8:17:c8:0b:08:4d: cd:45:fb:45:e3:e2:76:48:23:04:14:05:b4:b5:37: 1d:e0:05:cd:d6:45:bb:6e:55:01:b5:9c:48:6d:6f: 63:85:3c:76:4a:2d:04:98:8b:f9:14:71:96:f7:1e: b8:58:86:37:e7:60:12:18:31:23:0e:05:fe:04:8b: cf:d3:3f:8e:28:20:0e:ff:bc:b3:c8:ed:0e:48:7b: 2d:73:af:ee:d4:54:76:f6:ba:37:84:05:4c:5e:bc: d9:b9:7d:47:bb:b8:a2:f8:ff:07:f5:de:4a:0e:a8: 60:a0:18:30:dc:ef:8d:63:42

7.1.1.2 Certificate Extensions

Table 2. Certificate extensions — BalTstamp Root CA 2026

Extension	Required	Critical	Description	Value (from BalTstamp Root CA 2026)
Subject Key Identifier (2.5.29.14)	Yes	No	Identifies certificates containing this public key	A0:26:EE:F5:71:2C:F6:82: D6:FC:EA:E7:B5:5A:81:66: 05:7E:7A:AB
Basic Constraints (2.5.29.19)	Yes	Yes	Identifies the certificate as a CA certificate and sets max path depth	cA: TRUE pathlen: 1
Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key	Certificate Sign CRL Sign

7.1.2. Issuing CA Certificate Profile

The Issuing CA (Intermediate CA) certificate is signed by the Root CA. It acts as the operational issuing authority for TSU certificates and OCSP Responder certificates. pathLenConstraint = 0 ensures no further subordinate CAs may be chained beneath it.

7.1.2.1 Certificate Fields

Table 3. Certificate fields — BalTstamp Issuing CA 2026 G3

Field	Required	Description	Value (from BalTstamp Issuing CA 2026 G3)
Version	Yes	X.509 version of the encoded certificate	Version 3 (0x2)
Serial Number	Yes	Positive integer assigned by the TSA	08:21:5c:78:5e:5f:86:da:81:67: 5a:2f:42:1a:e6:76:65:9e:29:42
Issuer DN	Yes	Entity that signed and issued the certificate (Root CA)	C = LT O = Baltstamp UAB CN = BalTstamp Root CA 2026 organizationIdentifier = NTRLT-302608545
Subject DN	Yes	Entity associated with the public key	C = LT O = BalTstamp UAB CN = BalTstamp Issuing CA 2026 G3 organizationIdentifier = NTRLT-302608545
Not Before	Yes	Start of the certificate validity period	Jun 9 12:32:45 2026 GMT
Not After	Yes	End of the certificate validity period	Jun 6 12:32:45 2036 GMT (10 years)
Signature Algorithm	Yes	Algorithm used to sign the certificate	ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Subject Public Key Algorithm	Yes	Public key algorithm identifier	id-ecPublicKey (OID: 1.2.840.10045.2.1)
Elliptic Curve	Yes	Named elliptic curve used for the public key	brainpoolP512r1 (512-bit)
Public Key (partial)	Yes	Subject public key value	04:1f:ee:14:57:43:2c:84:62:32:69:c2:d7:d5:9f: 5e:b5:d3:ba:70:db:d8:ab:25:86:b9:21:b9:3b:54: c7:e0:4f:25:b8:8f:2b:ec:9a:e2:fa:4f:08:00:a9: 2b:25:f9:e5:52:7f:de:06:92:0e:80:e2:55:0e:96: 75:49:37:0a:f1:95:46:2e:42:eb:8d:5a:cc:55:e4: b1:c9:0d:d3:fa:de:08:3e:2f:8b:05:36:32:99:31: 49:9b:cb:ae:1a:27:d7:68:90:95:ed:b1:dd:c6:73: c0:7e:77:1f:e3:88:a9:0c:eb:ee:ee:3d:04:70:1e: dd:f9:40:bf:0f:bf:b0:e2:dc

7.1.2.2 Certificate Extensions

Table 4. Certificate extensions — BalTstamp Issuing CA 2026 G3

Extension	Required	Critical	Description	Value (from BalTstamp Issuing CA 2026 G3)
Subject Key Identifier (2.5.29.14)	Yes	No	Identifies certificates containing this public key	94:6E:A8:45:28:0F:A6:68: C2:71:00:14:B8:58:75:37: A8:6B:8D:EB
Authority Key Identifier (2.5.29.35)	Yes	No	Identifies the public key of the issuer (Root CA)	A0:26:EE:F5:71:2C:F6:82: D6:FC:EA:E7:B5:5A:81:66: 05:7E:7A:AB
Basic Constraints (2.5.29.19)	Yes	Yes	Identifies as CA; max path depth 0 (no subordinate CAs)	cA: TRUE pathlen: 0
Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key	Certificate Sign CRL Sign
Authority Information Access (1.3.6.1.5.5.7.1.1)	Yes	No	Indicates how to access information and services for the issuer	CA Issuers: http://pki-ec.baltstamp.lt/baltstamp-root-ca-ec.crt
CRL Distribution Points (2.5.29.31)	Yes	No	Identifies how CRL information is obtained	http://pki-ec.baltstamp.lt/baltstamp-root-ca-ec.crl
Certificate Policies (2.5.29.32)	Yes	No	Certificate policy OID and qualifier	Policy: X509v3 Any Policy

7.1.3. TSU Certificate Profile — TSU3

TSU certificates are issued by the Issuing CA and are used exclusively for signing qualified electronic time stamps.

7.1.3.1 Certificate Fields

Table 5. Certificate fields — BalTstamp QTSA TSU3

Field	Required	Description	Value (from BalTstamp QTSA TSU3)
Version	Yes	X.509 version of the encoded certificate	Version 3 (0x2)
Serial Number	Yes	Positive integer assigned by the TSA	2e:84:e8:58:36:42:57:33:54:3c: 6c:d0:a9:5c:20:3c:73:53:2f:4a
Issuer DN	Yes	Entity that signed and issued the certificate (Issuing CA)	C = LT O = BalTstamp UAB CN = BalTstamp Issuing CA 2026 G3 organizationIdentifier = NTRLT-302608545
Subject DN	Yes	Entity associated with the public key	C = LT L = Vilnius O = BalTstamp UAB CN = BalTstamp QTSA TSU3 organizationIdentifier = NTRLT-302608545
Not Before	Yes	Start of the certificate validity period	Jun 9 12:55:05 2026 GMT
Not After	Yes	End of the certificate validity period	Jun 8 12:55:05 2031 GMT (5 years)
Signature Algorithm	Yes	Algorithm used to sign the certificate	ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Subject Public Key Algorithm	Yes	Public key algorithm identifier	id-ecPublicKey (OID: 1.2.840.10045.2.1)
Elliptic Curve	Yes	Named elliptic curve used for the public key	brainpoolP384r1 (384-bit)
Public Key (partial)	Yes	Subject public key value	04:1c:a0:05:58:4d:91:57:d0:37:6e:17:94:07:fe: ee:9f:2c:f1:5d:dc:64:7d:2d:c8:63:67:26:4b:33: 00:fe:c3:2e:4c:b4:fc:04:e4:ef:b0:92:83:8f:1b:

			3f:95:ca:56:1f:38:c5:48:01:d2:28:42:eb:14:d3: 2f:7f:c9:fb:c3:67:a4:46:58:96:59:85:ae:d3:2b: 8d:64:10:40:27:b0:9e:4c:18:76:7d:8d:7b:80:86: b7:62:c2:b3:23:2e:dd
--	--	--	---

7.1.3.2 Certificate Extensions

Table 6. Certificate extensions — BalTstamp QTSA TSU3

Extension	Required	Critical	Description	Value (from BalTstamp QTSA TSU3)
Basic Constraints (2.5.29.19)	No	Yes	Confirms this is not a CA certificate	cA: FALSE
Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key	Digital Signature Non Repudiation
Extended Key Usage (2.5.29.37)	Yes	Yes	Time-stamping purpose for the certified public key	id-kp-timeStamping (1.3.6.1.5.5.7.3.8) Time Stamping
Subject Key Identifier (2.5.29.14)	Yes	No	Identifies certificates containing this public key	87:14:AB:FD:BD:E3:BE:B1: E6:20:BD:5C:13:97:2E:47: 2F:C2:0B:89
Authority Key Identifier (2.5.29.35)	No	No	Identifies the public key of the issuer (Issuing CA)	94:6E:A8:45:28:0F:A6:68: C2:71:00:14:B8:58:75:37: A8:6B:8D:EB
Authority Information Access (1.3.6.1.5.5.7.1.1)	Yes	No	Indicates how to access information and services for the issuer	OCSP: http://ocsp-ec-intermediate.baltstamp.it CA Issuers: http://pki-ec.baltstamp.it/baltstamp-issuing-ca-ec.crt
CRL Distribution Points (2.5.29.31)	Yes	No	Identifies how CRL information is obtained	http://pki-ec.baltstamp.it/baltstamp-issuing-ca-ec.crl
Certificate Policies (2.5.29.32)	Yes	No	Certificate policy OIDs and CPS qualifier URL	Policy: 0.4.0.2042.1.2 Policy: 1.3.6.1.4.1.38424.1.2.1 CPS: http://www.baltstamp.it/

7.1.4. TSU Certificate Profile — TSU4

TSU4 is the secondary time-stamping unit. Its certificate profile is identical to TSU3. Both TSUs are active and available for time-stamp generation.

7.1.4.1 Certificate Fields

Table 7. Certificate fields — BalTstamp QTSA TSU4

Field	Required	Description	Value (from BalTstamp QTSA TSU4)
Version	Yes	X.509 version of the encoded certificate	Version 3 (0x2)
Serial Number	Yes	Positive integer assigned by the TSA	29:3f:68:ac:bf:cd:d9:8e:e6:d6: 96:1b:74:43:3b:13:e2:6e:c0:04
Issuer DN	Yes	Entity that signed and issued the certificate (Issuing CA)	C = LT O = BalTstamp UAB CN = BalTstamp Issuing CA 2026 G3 organizationIdentifier = NTRLT-302608545
Subject DN	Yes	Entity associated with the public key	C = LT L = Vilnius O = BalTstamp UAB CN = BalTstamp QTSA TSU4 organizationIdentifier = NTRLT-302608545
Not Before	Yes	Start of the certificate validity period	Jun 9 12:56:27 2026 GMT
Not After	Yes	End of the certificate validity period	Jun 8 12:56:27 2031 GMT (5 years)
Signature Algorithm	Yes	Algorithm used to sign the certificate	ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Subject Public Key Algorithm	Yes	Public key algorithm identifier	id-ecPublicKey (OID: 1.2.840.10045.2.1)
Elliptic Curve	Yes	Named elliptic curve used for the public key	brainpoolP384r1 (384-bit)
Public Key (partial)	Yes	Subject public key value	04:5d:b3:4f:47:c1:7a:10:e3:3d:e1:58:34:15:a1: 60:23:0e:fb:fc:e4:88:9e:29:b2:44:9a:eb:f6:66: 2c:a7:42:4e:17:9f:f1:16:99:87:7b:95:dd:1b:a7: 1a:43:dd:2d:52:f1:9b:63:1a:11:25:2e:9a:87:be: eb:f2:48:0b:8e:d0:1e:09:46:61:e9:70:68:3e:9a: 7e:08:c4:fa:b9:78:ea:52:b0:14:bc:b2:62:9d:cc: 2b:59:11:2f:82:99:d3

7.1.4.2 Certificate Extensions

Table 8. Certificate extensions — BalTstamp QTSA TSU4

Extension	Required	Critical	Description	Value (from BalTstamp QTSA TSU4)
Basic Constraints (2.5.29.19)	No	Yes	Confirms this is not a CA certificate	cA: FALSE
Key Usage (2.5.29.15)	Yes	Yes	Defines the purpose of the key	Digital Signature Non Repudiation
Extended Key Usage (2.5.29.37)	Yes	Yes	Time-stamping purpose for the certified public key	id-kp-timeStamping (1.3.6.1.5.5.7.3.8) Time Stamping
Subject Key Identifier (2.5.29.14)	Yes	No	Identifies certificates containing this public key	18:9C:F9:92:10:AB:E3:CE: B5:C4:0A:C2:E6:86:1E:B7: D9:5C:EA:87
Authority Key Identifier (2.5.29.35)	No	No	Identifies the public key of the issuer (Issuing CA)	94:6E:A8:45:28:0F:A6:68: C2:71:00:14:B8:58:75:37: A8:6B:8D:EB
Authority Information	Yes	No	Indicates how to access information and services	OCSP: http://ocsp-ec-intermediate.baltstamp.lt

Access (1.3.6.1.5.5.7.1.1)			for the issuer	CA Issuers: http://pki-ec.baltstamp.it/baltstamp-issuing-ca-ec.crt
CRL Distribution Points (2.5.29.31)	Yes	No	Identifies how CRL information is obtained	http://pki-ec.baltstamp.it/baltstamp-issuing-ca-ec.crl
Certificate Policies (2.5.29.32)	Yes	No	Certificate policy OIDs and CPS qualifier URL	Policy: 0.4.0.2042.1.2 Policy: 1.3.6.1.4.1.38424.1.2.1 CPS: http://www.baltstamp.it/

7.2. CRL Profiles

BalTstamp TSA issues Certificate Revocation Lists in accordance with RFC 5280. Two CRLs are maintained: one signed by the Root CA (covering Issuing CA certificates) and one signed by the Issuing CA (covering TSU certificates). Regular CRL for Issuing certificate is published at least every 24 hours.

7.2.1. Root CA CRL Profile

The Root CA CRL is signed by the Root CA private key and lists any revoked Issuing CA certificates. It has a maximum validity of 365 days.

7.2.1.1 CRL Fields

Field	Required	Description	Value (Root CA CRL)
Version	Yes	Version of the encoded CRL	Version 2 (0x1)
Signature Algorithm	Yes	Algorithm used by the CRL issuer to sign the CRL	ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Issuer Name	Yes	Entity that signed and issued the CRL (Root CA)	C = LT O = Baltstamp UAB CN = BalTstamp Root CA 2026 organizationIdentifier = NTRLT-302608545
This Update	Yes	Issue date of this CRL	Jun 10 07:41:47 2026 GMT
Next Update	Yes	Date by which the next CRL will be issued (max 365 days)	Jun 10 07:41:47 2027 GMT
Revoked Certificates	No	List of revoked certificate serial numbers, revocation dates and reason codes	1 entry — see Section 7.2.1.3
Signature Value	Yes	Digital signature over the ASN.1 DER encoded tbsCertList	30:81:85:02:41:00:89:fb:91:78:84:a8:eb:1a:08:02:51:64:2f:96:61:5c:94:8c:6a:04:31:fa:ce:61:a8:8d:c8:b6:9a:5d:0e:5b:9f:0d:67:5f:a9:77:65:13:a1:a2:ae:4b:24:33:c1:14:a8:31:df:40:7c:37:b2:6c:ae:74:2c:43:73:50:ff:0a:02:40:68:67:4d:88:50:6b:55:6d:97:f1:f7:fa:38:fc:9f:45:7e:07:77:ae:55:fb:64:df:0c:7a:7f:7d:01:fa:4b:7a:56:21:57:09:f0:eb:21:84:86:c9:b4:ac:67:d0:e5:2a:9f:93:8e:0f:62:52:ff:3a:97:f8:af:8f:f6:54:a3:fd

o
t CA CRL (CRL Number: 13)

7.2.1.2 CRL Extensions

Table 14. CRL extensions — Root CA CRL (CRL Number: 13)

Extension	Required	Critical	Description	Value (Root CA CRL)
Authority Key Identifier (2.5.29.35)	Yes	No	Identifies the public key of the Root CA that signed this CRL	A0:26:EE:F5:71:2C:F6:82: D6:FC:EA:E7:B5:5A:81:66: 05:7E:7A:AB
CRL Number (2.5.29.20)	Yes	No	Monotonically increasing sequence number for this CRL scope and issuer	13

7.2.2. Issuing CA CRL Profile

The Issuing CA CRL is signed by the Issuing CA private key and covers the revocation status of TSU certificates.

7.2.2.1 CRL Fields

Table 16. CRL fields — Issuing CA CRL (CRL Number: 18)

Field	Required	Description	Value (Issuing CA CRL)
Version	Yes	Version of the encoded CRL	Version 2 (0x1)
Signature Algorithm	Yes	Algorithm used by the CRL issuer to sign the CRL	ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Issuer Name	Yes	Entity that signed and issued the CRL (Issuing CA)	C = LT O = BalTstamp UAB CN = BalTstamp Issuing CA 2026 G3 organizationIdentifier = NTRLT-302608545
This Update	Yes	Issue date of this CRL	Jun 11 02:30:02 2026 GMT
Next Update	Yes	Date by which the next CRL will be issued (max 7 days)	Jun 18 02:30:02 2026 GMT
Revoked Certificates	No	List of revoked TSU certificate serial numbers	1 entry — see Section 7.2.2.3
Signature Value	Yes	Digital signature over the ASN.1 DER encoded tbsCertList	30:81:84:02:40:54:4a:75:c0:93:dd:ca:8c:ee:77:3e:9a:18: ed:71:36:79:06:ac:0a:03:9d:cc:ec:7f:01:b0:59:f1:1e:93: fd:ee:fe:1e:40:41:45:b7:9c:e0:cd:b0:56:4d:3d:d7:aa:ed: 7a:e7:f6:70:79:6c:0c:6f:84:ee:38:e2:1e:93:fc:02:40:1b: 60:2b:7d:d5:fb:04:27:6b:be:a6:4e:49:b1:89:11:1b:d6:90: 45:31:c1:be:34:b5:43:0c:00:7f:6d:27:76:59:ac:86:e3:af: e0:92:61:6c:75:d3:3c:5c:c9:81:69:f3:64:17:de:5b:ce:c0: 3c:64:f1:85:13:34:85:f3:10

7.2.2.2 CRL Extensions

Table 17. CRL extensions — Issuing CA CRL (CRL Number: 18)

Extension	Required	Critical	Description	Value (Issuing CA CRL)
Authority Key Identifier (2.5.29.35)	Yes	No	Identifies the public key of the Issuing CA that signed this CRL	94:6E:A8:45:28:0F:A6:68: C2:71:00:14:B8:58:75:37: A8:6B:8D:EB
CRL Number (2.5.29.20)	Yes	No	Monotonically increasing sequence number for this CRL scope and issuer	18

7.3. OCSF Responder Certificate profile

The Intermediate OCSF Responder certificate is signed by the Issuing CA and provides revocation status for TSU certificates.

7.1.6.1 Certificate Fields

Table 11. Certificate fields — BalTstamp Intermediate OCSF Responder 2026 G3

Field	Required	Description	Value (BalTstamp Intermediate OCSF Responder 2026 G3)
Version	Yes	X.509 version	Version 3 (0x2)
Serial Number	Yes	Positive integer assigned by the TSA	1e:07:fb:a4:87:06:4c:bc:39:d8: eb:94:06:5a:ee:48:25:94:83:a1
Issuer DN	Yes	Signed by Issuing CA	C = LT O = BalTstamp UAB CN = BalTstamp Issuing CA 2026 G3 organizationIdentifier = NTRLT-302608545
Subject DN	Yes	OCSF Responder identity	C = LT O = BalTstamp UAB CN = BalTstamp Intermediate OCSF Responder 2026 G3 organizationIdentifier = NTRLT-302608545
Not Before	Yes	Start of validity period	Jun 9 12:35:52 2026 GMT
Not After	Yes	End of validity period (5 years)	Jun 8 12:35:52 2031 GMT
Signature Algorithm	Yes	Algorithm	ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Elliptic Curve	Yes	Named curve	brainpoolP384r1 (384-bit)

7.1.6.2 Certificate Extensions

Table 12. Certificate extensions — BalTstamp Intermediate OCSF Responder 2026 G3

Extension	Required	Critical	Description	Value (Intermediate OCSF Responder 2026 G3)
Basic Constraints (2.5.29.19)	Yes	Yes	Not a CA certificate	cA: FALSE
Key Usage (2.5.29.15)	Yes	Yes	Digital signature only	Digital Signature
Extended Key Usage (2.5.29.37)	Yes	No	OCSF signing purpose	OCSF Signing
Subject Key Identifier (2.5.29.14)	Yes	No	Subject public key hash	C3:C8:66:53:CF:EA:46:92: 3F:B3:C7:82:7E:19:CA:1A: 9A:DF:EF:E4
Authority Key Identifier (2.5.29.35)	Yes	No	Issuing CA public key hash	94:6E:A8:45:28:0F:A6:68: C2:71:00:14:B8:58:75:37: A8:6B:8D:EB
OCSF No Check (1.3.6.1.5.5.7.48.1.5)	Yes	No	Relying parties need not check revocation status of this cert	(present)

8.COMPLIANCE AUDIT AND OTHER ASSESSMENTS

To ensure that the requirements of this CPPS are being implemented and enforced and to be act upon according to requirement and recommendations stated in REGULATION (EU) No 910/2014 [1] and ISO 27001 - ISO/IEC 27001 [6] the TSP is having conformity assessment both internal and external. These are held on a regular basis and may be held when requested both from the organization it selves or from authorized external parties.

The conformity assessment is held by a conformity assessment body approved by the supervisory body in the relevant EU/EEA member state as stated in REGULATION (EU) No 910/2014 [2]. The Communications Regulatory Authority of the Republic of Lithuania is the conformity assessment body for the TSP.

The TSP has a defined review process for this CPPS which including responsibilities for maintaining the TSP practice statement and policy.

8.1 Frequency or Circumstances of Assessment

The TSP are audited at least every 24 months by a conformity assessment body. The purpose of the audit is to confirm that the TSP as a qualified trust service provider and the qualified trust services provided by the TSP fulfil the requirements laid down in REGULATION (EU) No 910/2014 [2]. The TSP submits the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

In accordance with REGULATION (EU) No 910/2014 [2] article 20, the TSP accept the supervisory body (or a conformity body upon the supervisory request) upon request to perform audits at all time, to confirm the TSP fulfil its scope to be according to the requirements laid down in REGULATION (EU) No 910/2014 [2]

Where personal data protection rules appear to have been breached, the supervisory body informs the data protection authorities of the results of its audits.

8.2 Identity/Qualifications of Assessor

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

The TSP and the conformity assessment body are independent of each other.

8.4 Topics Covered by Assessment

Within the scope of the TSP's CPPS the REGULATION (EU) No 910/2014 [1], ISO 27001 - ISO/IEC 27001 [6] and ETSI EN 319 411-1 [3] is covered by assessment.

8.5 Actions Taken as a Result of Deficiency

Finding of deficiencies in assessment are treated promptly and according to the TSP internal procedure for internal and external audits.

8.6 Communication of Results

The supervisory body Communications Regulatory Authority of the Republic of Lithuania is entitled to see the results of the assessment from the conformity Assessment Body. The TSP sends the result of the assessment to the supervisory body no later than three days after receiving the result from the conformity assessment body.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Not Applicable.

9.2 Financial Responsibility

Not Applicable.

9.3 Confidentiality of Business Information

No stipulation

9.4 Privacy of Personal Information

Not Applicable.

9.5 Intellectual Property Rights

Not Applicable.

9.6 Representations and Warranties

Not Applicable.

9.7 Disclaimers of Warranties

Not Applicable.

9.8 Limitations of Liability

Not Applicable.

9.9 Indemnities

Not Applicable.

9.10 Term and TerminationLimitations of Liability

Not Applicable.

9.11 Individual Notices and Communications with Participants

Not Applicable.

9.12 Amendments

The TSP notify notice of changes it intends to make in its practice statement and, following approval as in section “1.5. Policy administration” and make the revised TSP practice statement immediately available. The notify notice of change is at least given to the supervisory body and is given prior to the intended change.

9.12.1 Procedure for Amendment

Any changes to this CPPS must be approved by the director of the BalTstamp according to

section “1.5. Policy administration”. If a change in the CPPS results in a new OID version, new certificates issued will have this new OID version referenced to.

Updates supersede any designated or conflicting provisions of the referenced version of the CPPS.

9.12.2 Procedure for Amendment Notification Mechanism and Period

The TSP notifies its supervisory body and the conformity assessment body upon intended changes to its CPPS and if applicable affected parties. The TSP reserves the right to amend this CPPS without notification to end-users.

By using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance is required to be confirmed by the conformity assessment body.

9.12.3 Circumstances Under Which OID Must be Changed

In general, changes to this CPPS result in a new OID version for the effected certificate. If changes not materially reduce the assurance that a CPPS or its implementation provides, and are judged by the UAB Baltstamp director to have an insignificant effect on the acceptability of certificates, then change in the CP OID are not required. Changes in the CPPS that materially change the acceptability of certificates for one or more specific purposes requires corresponding changes to the CP OID.

9.13 Dispute Resolution Provisions

Not Applicable.

9.14 Governing Law

Not Applicable.

9.15 Compliance with Applicable Law

Not Applicable.

9.16 Miscellaneous Provisions

Not Applicable.

9.17 Other Provisions

Not Applicable.

10. 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.
- [EN 319 401] - ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- [EN 319 411-1] - ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- [EN 319 412-1] - ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- [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 319 421] - ETSI EN 319 421 Electronic Signatures and 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 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.[BalTstamp TSPS] BalTstamp Time-Stamping Practice Statement.

