Timestamp Root CA and TSA Certificate Policy and Certificate Practice Statement

CP: 1.3.171.5.3.2.1.1.0

CPS: 1.3.171.5.3.2.2.1.0

Version: 1.1
Classification: Restricted

Document history and validation cycle

Version	Description	Author	Reviewer	Document Status	Date of publication
1.0	Initial release of the document.	*Clément Gorlt, Director*	*Clement Gorlt, Director* *Mohamed Ismaili, Director*	*Published*	*23/05/2025*
1.1	Minor terminology correction: replaced “QSCD” with “HSM”	Shivam Singh, Manager	Clement Gorlt, Director	Published	09/06/2025

Table of content

1 INTRODUCTION

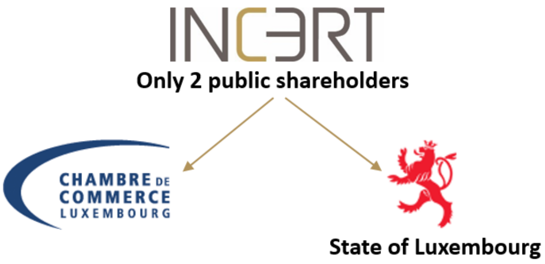
This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which this CP is targeted.

This document follows the framework and structure outlined in the Internet Engineering Task Force's RFC 3647.

1.1 Overview

Incert GIE has been founded in August 2012 by the State of Luxembourg and the Luxembourg Chamber of Commerce, and has initiated its establishment in January 2013 by integrating existing IT infrastructures within its organization and by deploying new ones.

Our current shareholding structure brings insurance to the continuity of our business services:



Within the aim to constantly improve its information security and operational activities, Incert GIE has established since the end of year 2013 the requirements defined in ISO/IEC 27001:2022 standard for all its business and internal services.

This document constitutes both the Certificate Policy (CP) and Certification Practice Statement (CPS) for the Timestamp Root Certification Authority (Timestamp Root CA) and Timestamp Authority (TSA) certificates. The Timestamp Root CA is established to issue and manage certificates solely for Timestamp Authorities (TSAs) that provide Qualified Electronic Timestamp Services in accordance with Regulation (EU) No 910/2014 (eIDAS) and applicable ETSI standards.

The Timestamp Root CA is a self-signed Root CA, which operates as a private trust hierarchy dedicated to qualified timestamping. Its sole purpose is to issue, maintain, and revoke the certificate of one or more timestamp authorities (TSAs). The Root CA undergoes conformity assessment audits by a Qualified Trust Service Auditor and is submitted for inclusion in the European Union Trust List (EUTL) following successful audit.

The TSA certificate issued under this Timestamp Root CA meets the requirements for qualified electronic time-stamps under Article 42 of Regulation (EU) No 910/2014 and is validated via inclusion of the Root CA in the EU Trusted List.

The timestamp tokens issued by the TSA(s) under this Root CA are expected to be used for long-term validation and legal acceptance of signed data, meeting the requirements for Qualified Electronic Timestamps under the eIDAS Regulation.

This combined CP/CPS document is designed to meet the requirements of ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates), particularly focusing on policies applicable to trust service providers supporting electronic signature or electronic seal creation.

The following OID identifies the policy under which the Timestamp Root CA operates and should appear in certificates issued by this Root CA: 1.3.171.5.3.2.2.1.0

1.2 Document Name and Identification

- Document Name: Timestamp Root CA and TSA Certificate Policy and Certification Practice Statement
- OID: See above
- Version: 1.1
- Status: Published
- Date of Issue: 09th June 2025

1.3 PKI Participants

1.3.1 Trust Service Provider (TSP)

Incert acts as a Qualified Trust Service Provider for timestamping under eIDAS. Incert is responsible for:

- Operating the Timestamp Root CA and issuing TSA certificate(s),
- Ensuring continuous compliance with ETSI standards and applicable legal requirements.

The Timestamp Root CA is a self-signed trust anchor operated by INCERT solely for the purpose of issuing timestamping certificates to the INCERT Timestamping Authority. It is not used for issuing end-user or subordinate CA certificates and does not serve as a general-purpose CA.

The Timestamp Root CA:

- Maintains a single active signing key pair, securely protected in an offline HSM,
- Is subject to external audits in compliance with ETSI EN 319 411-1,
- Is included in the EU Trusted List as a qualified trust anchor for timestamping services,

- Publishes its certificate, Certificate Policy (CP), and CRL in the public repository.

The TSA Root CA plays a foundational role in establishing legal and technical trust in the qualified timestamp tokens issued by the TSA.

1.3.2 Registration Authorities

The Timestamp Root CA performs RA functions internally, under strict procedural and personnel controls.

1.3.3 Subscribers

Subscribers for the Timestamp Root CA are Timestamp Authorities (TSAs) that receive certificates from the Root CA and are responsible for generating timestamp tokens.

Subscribers for the Incert TSA are entities (e.g., individuals, IT systems) that request time-stamp tokens for their data. Subscribers must be contractually affiliated with Incert and are responsible for:

- Submitting correct hash values
- Validating received tokens
- Ensuring integration by following agreed specifications

1.3.4 Relying Parties

Relying Parties are individuals or systems that rely on the cryptographic and temporal validity of a TST issued by Incert. They may include:

- An industry sector regulator,
- Legal professionals,
- System integrators and software vendors.

1.3.5 Other Participants

Supervisory Bodies and Qualified Trust Service Auditors play key roles in the assessment and trust inclusion of the Root CA.

1.4 Certificate Usage

This CP/CPS applies to Timestamp Root CA, for which the certificates:

- Issued by the Timestamp Root CA may only be used by TSAs to issue qualified timestamp tokens in accordance with eIDAS and relevant ETSI standards,
- Must not be used for signing user documents, email protection, client/server authentication, or code signing,
- Issued and maintained within HSMs.

But also, for the timestamping certificates used by Incert TSA, for which the certificate is:

- Used exclusively for signing TSTs issued under RFC 3161
- Not used for signing subscriber data, code, or documents, nor be used for identity, SSL/TLS, or document signing
- Issued and maintained within HSMs

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP and the documents referenced herein are maintained and administered by INCERT which can be contacted at:

INCERT GIE,
15 rue léon laval,
L-3372 Leudeulange
Grand-Duchy of Luxembourg

E-mail: pki@incert.lu
Web site: https://www.incert.lu

1.5.2 Contact Person

Questions regarding this CP shall be directed to the PKI team:

PKI team
INCERT GIE
15 rue léon laval,
L-3372 Leudeulange
Grand-Duchy of Luxembourg

E-mail: pki@incert.lu
Tel: (352) 273 267 1

1.5.3 Person Determining CP and CPS Suitability for the Policy

The ISMS oversight committee approves this CP and the subordinated CPS.

1.5.4 CP and CPS approval procedures

The ISMS oversight committee review any modifications, additions or deletions to the CPS and determine if these changes are acceptable. At their sole discretion, they must approve or reject any proposed changes of the CPS related to this CP.

1.6 Definitions and Acronyms

CA: Certification Authority

CPS: Certification Practice Statement

CP: Certificate Policy

CRL: Certificate Revocation List

eIDAS: Electronic Identification, Authentication and Trust Services Regulation

ETSI: European Telecommunications Standards Institute

OID: Object Identifier

PKI: Public Key Infrastructure

TSA: Timestamping Authority

TSP: Trust Service Provider

TST: Timestamp Token

(Full glossary and acronym list will be appended in Chapter 10.)

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repository Access

Incert publishes the following information in its publicly accessible repository:

- The Root CA certificate,
- Certificate Revocation Lists (CRLs) issued by the Root CA,
- This CP/CPS document and its updates,
- Audit reports and other applicable compliance documentation (when approved for publication).

The URL for the repository is following:

- https://repository.incert.lu/

2.2 Publication of Certification Information

The Timestamp Root CA ensures timely publication of the following information:

- The self-signed Timestamp Root CA certificate,
- CRLs issued by the Root CA, with a maximum validity of 6 months and regular updates to ensure revocation information remains available,
- Updates or modifications to this CP/CPS document,
- Contact details for the TSP and reporting mechanisms for suspected key compromise or operational incidents.

Information published in the repository is freely available and accessible to relying parties and auditors.

2.3 Time or Frequency of Publication

- Root CA Certificate: Published immediately upon creation and remains available as long as the CA is active or until all certificates it issued have expired or been revoked,
- CRLs: Published at regular intervals not exceeding 2 months and immediately upon certificate revocation,
- CP/CPS: Published upon initial approval and upon each substantive revision,
- Audit Reports: Published following approval by the supervising body, if required.

2.4 Access Controls

The repository is accessible to the public without restrictions for reading the published content.

Write access to the repository is strictly controlled and limited to authorized personnel under change management procedures. Integrity of published data is protected using appropriate technical and procedural controls.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The Timestamp Root CA and all issued certificates use X.500 Distinguished Names (DNs) as defined in RFC 5280. The names are structured to ensure unambiguous identification of the CA.

The DN of the Timestamp Root CA certificate includes the following attributes:

- countryName (C),
- organizationName (O),
- commonName (CN),
- organizationIdentifier.

Since timestamping services does not involve subject identity or certificate issuance to individuals, traditional naming and identity proofing are not applicable at the token level. However, the following applies:

- Each **TSA** certificate is uniquely named and identified using an X.500 Distinguished Name (DN)
- The TSA DN is included in each TST issued

3.1.2 Need for Names to be Meaningful

The DN attributes are selected to be meaningful and to clearly identify the entity (INCERT) operating the Timestamp Root CA in accordance with applicable policy and legal requirements.

3.1.3 Anonymity or Pseudonymity of Subscribers

Not applicable. The Timestamp Root CA does not issue end-entity certificates to natural persons or pseudonymous identities. It only issues certificates to Timestamp Authorities.

3.1.4 Rules for Interpreting Various Name Forms

Naming conventions follow applicable ETSI and RFC standards. No local naming conventions beyond those are used.

3.1.5 Uniqueness of Names

The Timestamp Root CA ensures that the DN of each certificate it issues is unique within its namespace.

3.1.6 Recognition, Authentication, and Role of Trademarks

The CA operator ensures that the names used in certificates do not violate intellectual property or trademark rights.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Timestamp Root CA proves possession of the private key during self-signed certificate generation and through the secure operation of cryptographic modules (e.g., HSMs).

3.2.2 Authentication of Organization Identity

The Timestamp Root CA is operated by an identified organization. Prior to inclusion in the EU Trust List and recognition as a Qualified Trust Service Provider, the organization undergoes:

- Verification of legal identity,
- Validation of operational readiness,
- Conformance to applicable audit requirements (e.g., ETSI EN 319 403).

3.2.3 Authentication of Individual Identity

Not applicable. The Root CA is not associated with a natural person.

3.2.4 Non-Verified Subscriber Information

Not applicable. The Root CA does not issue subscriber certificates to natural persons. The only subscribers are TSA authorities which are identified and authenticated using internal procedures.

3.2.5 Validation of Authority

INCERT provides documented evidence of authorization to act as the Certification Authority, including official registration and mandate to provide trust services.

3.2.6 Criteria for Interoperation

The Root CA may interoperate with other infrastructures (e.g., EU Trust List, QTSP ecosystems) only after successful audit and supervisory authority approval.

3.2.7 Initial subscriber Validation for timestamping services

Before being granted access to the timestamping service:

- Subscribers undergo contractual onboarding
- Identity and affiliation of the organization are verified
- Technical integration requirements are confirmed
- Authorization to submit timestamp requests is established§

3.2.8 Key possession and validation for timestamping services

TSA private keys are securely generated and stored in a certified HSM by Incert. The possession of these keys is verified internally, under dual control, and during compliance audits. Incert remains the custodian of timestamp keys.

Subscribers are not required to generate or hold any cryptographic keys related to the timestamping function.

3.3 Identification and Authentication for Re-Key-Requests

Re-keying of the Root CA certificate is planned well in advance and is conducted under strict security controls, including generation in a secure environment and issuance of a new self-signed certificate.

The same security requirement applies for rekeying of the TSA certificate.

3.4 Identification and Authentication for Revocation Requests

Revocation of the Root CA certificate is an exceptional event and would be initiated only under critical circumstances such as key compromise or cessation of service. Requests must originate from authorized personnel and be validated through multi-factor administrative controls.

4 Certificate Life-Cycle and TSA Operational Requirements

This section defines the procedures and requirements involved throughout the lifecycle of certificates issued by the Timestamp Root CA, including certificate application, issuance, acceptance, use, renewal, modification, rekey, suspension (if applicable), revocation, and status checking services. These practices are consistent with ETSI EN 319 411-1 requirements for a qualified trust service provider (QTSP) operating a Certification Authority (CA) intended to issue qualified certificates to a Time-Stamping Authority (TSA). As well as the operational activities undertaken by Incert TSA to ensure the secure, reliable, and standards-compliant issuance of time-stamp tokens (TSTs). These activities are essential to establishing temporal evidence that can be used for long-term data integrity, legal proof, and regulatory compliance—particularly in the context of relying party applications

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Only authorized personnel within the Trust Service Provider (TSP) INCERT, specifically designated to manage the lifecycle of the Timestamp Authority, are permitted to submit certificate requests to the Timestamp Root CA. No external entities or third parties are allowed to request certificates from the Timestamp Root CA.

4.1.2 Enrollment process and responsibilities

The certificate application for the TSA certificate must be initiated in accordance with the internal Certificate Signing Request (CSR) generation procedure. The private key associated with the TSA must be generated and held in a certified Hardware Security Module (HSM), and the CSR must comply with the defined subject DN, key usage, and certificate policy OID(s) associated with qualified TSA certificates. Internal dual control procedures are employed to authorize and approve each certificate request. The Timestamp Root CA will log all relevant events and maintain an auditable trail for the request process.

4.2 Certificate Application Processing

4.2.1 Performing identification and authentication functions

Since the applicant is the internal TSA component, the Timestamp Root CA relies on internally validated roles and security processes to authenticate the certificate request. These include verifying the integrity of the CSR, confirming that the request originated from a trusted certified Hardware Security Module (HSM), and ensuring that the requesting entity is an approved component within the organizational PKI hierarchy.

More generally, the TSA key and CSR are generated as part of a key ceremony with witness in order to guarantee the certificate is generated and used in a controlled way.

4.2.2 Approval or rejection of certificate applications

Applications for a TSA certificate are subject to a formal approval process, which includes validation of the CSR attributes, approval from designated CA personnel, and audit trail creation. Applications that do not comply with predefined technical and organizational requirements are rejected, and the rejection is recorded in the CA logs.

4.2.3 Time to process certificate applications

Certificate applications shall be processed in a timely manner, typically within one business day following approval. The issuance timeframe may be extended based on internal security checks or technical validation requirements.

4.3 Certificate Issuance

4.3.1 CA actions during certificate issuance

The authorized personnel at INCERT responsible for Timestamp Root CA performs the following actions during issuance:

- Validates the CSR against internal policies,
- Ensures the certificate content is compliant with ETSI requirements (e.g., ETSI EN 319 411-1, 319 421),
- Signs the certificate using the Timestamp Root CA's private key in a secured and audited environment,
- Associates the certificate with the correct certificate policy OID(s),
- Ensures logging of issuance details and stores the certificate in the CA repository.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Since the subscriber is an internal component (the TSA), issuance is confirmed via secure internal procedures and acknowledged through system-level logs and documentation. The issued certificate is imported into the TSA's Certified Hardware Security Module (HSM) in a controlled manner and under the supervision of authorized personnel.

4.4 Certificate Acceptance

4.4.1 Conduct certificate acceptance

Certificate acceptance is considered to occur when:

- The issued TSA certificate is successfully imported into the TSA system’s Certified Hardware Security Module (HSM) by authorized personnel,
- The certificate is actively used to sign Time-Stamp Tokens (TSTs) or otherwise becomes operational within the production environment,
- Internal audit logs reflect the completion of the acceptance procedure, and an entry is made in the certificate lifecycle documentation.

By conducting these activities, the TSP acknowledges that:

- The certificate content (e.g., subject DN, key usages, policy OIDs) has been verified and found correct,
- The associated private key is securely held in accordance with applicable regulations,
- All responsibilities related to the TSA certificate lifecycle are understood and accepted.

4.4.2 Publication of the certificate by the CA

The issued TSA certificate is published in the CA’s public certificate repository. This repository is accessible through an HTTP endpoint and contains:

- The TSA certificate (in DER format),
- The Timestamp Root CA certificate,
- Any applicable CRLs issued by the CA.

4.4.3 Notification of certificate issuance by the CA to other entities

As the Root CA and TSA are components of the same TSP infrastructure, no external notification is typically required. However, relevant information (e.g., certificate serial number, issuance time) is logged and may be made available to the supervisory body or conformity assessment body upon request.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

The TSA private key associated with the certificate issued by the Timestamp Root CA is restricted to the generation of qualified electronic timestamps, in accordance with:

- ETSI EN 319 421,
- The CP/CPS of the TSA and Timestamp Root CA,
- The constraints encoded in the certificate itself (e.g., key usage = digitalSignature, extended key usage = timeStamping).

The private key must be stored and used exclusively within a Certified Hardware Security Module (HSM), and any operation using this key must be authorized and logged.

4.5.2 Relying party public key and certificate usage

Relying parties are authorized to use the TSA certificate for the sole purpose of validating Timestamp Tokens issued under this certificate. They must rely on the public key and associated certificate chain only within the context of:

- Trusting timestamps that conform to eIDAS Regulation and ETSI standards,
- Verifying signature integrity and timestamp authenticity.

Usage outside the defined scope is not permitted and disclaimed by the CA.

4.6 Certificate Renewal

4.6.1 Circumstance for certificate renewal

Certificate renewal may occur when:

- The certificate is approaching its expiration, and the associated private key remains uncompromised and valid for continued use,
- There is a need to extend the operational validity without modifying subject information or key material.

4.6.2 Who may request renewal

Only authorized personnel within the TSP can initiate the renewal request, subject to internal policy and dual-control approval.

4.6.3 Processing certificate renewal requests

The renewal request is subject to the same technical and procedural validation as an initial application. The renewed certificate must preserve the integrity and continuity of the TSA's operations, and any deviations must be documented and approved.

4.6.4 Notification of new certificate issuance to subscriber

The renewed certificate is delivered securely to the authorized TSA personnel. Installation and activation follow internal documented procedures.

4.6.5 Conduct acceptance of a renewed certificate

The same conditions outlined in 4.4.1 apply to the acceptance of a renewed certificate.

4.6.6 Publication of the renewal certificate by the CA

Renewed certificates are published in the same public repository alongside the original.

4.6.7 Notification of certificate issuance by the CA to other entities

Same as 4.4.3; generally, no external notification unless required by the supervisory body.

4.7 Certificate Re-Key

4.7.1 Circumstance for certificate re-key

Certificate re-key may occur under the following conditions:

- The private key associated with the TSA certificate is due for rotation as part of a scheduled cryptoperiod rollover,
- The cryptographic strength of the key is no longer deemed sufficient (e.g., due to evolving threat models or industry guidelines),
- The private key is suspected of compromise, but the TSA operations can be restored using a newly generated key pair without requiring revocation of the Root CA certificate.

4.7.2 Who may request certification of a new public key

Only designated and authorized TSP personnel may initiate a certificate re-key request. This request must be approved by the ISMS oversight committee and supported by a documented justification.

4.7.3 Processing certificate re-keying requests

The re-keying process involves:

- Generating a new key pair using the same Hardware Security Module (HSM) as the original or a newly certified HSM,
- Submission of a new Certificate Signing Request (CSR) to the Timestamp Root CA,
- Review of the request by Root CA personnel in accordance with established authentication and approval procedures,
- Issuance of a new TSA certificate with updated key material and validity dates, maintaining the same policy OIDs and operational scope.

4.7.4 Notification of new certificate issuance to subscriber

Upon successful issuance, the new certificate is securely installed by authorized personal. The transition is coordinated to ensure continuity of timestamping operations and proper decommissioning of the old key pair if applicable.

4.7.5 Conduct acceptance of a re-keyed certificate

The acceptance procedures described in Section 4.4.1 apply similarly to re-keyed certificates. Internal logs and change management records must reflect the event.

4.7.6 Publication of the re-keyed certificate by the CA

The re-keyed certificate is published in the same repository, clearly distinguishable by serial number and issuance date. Associated metadata is also updated.

4.7.7 Notification of certificate issuance by the CA to other entities

Unless required by regulatory or supervisory bodies, no external notification is typically issued. The new certificate is published and all relevant lifecycle events are documented.

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

Certificate modification is limited to minor non-security impacting changes, such as:

- Typographical corrections in subject information (if permitted),
- Updates to non-critical extensions, where allowed by policy.

However, due to the strict requirements for qualified trust service certificates, such modifications are rare. Most scenarios instead necessitate re-keying or full re-issuance.

4.8.2 Who may request certificate modification

Only designated TSP personnel may request a modification, subject to change control procedures and dual control approval.

4.8.3 Processing certificate modification requests

Requests are reviewed by the Timestamp Root CA in accordance with internal policy. If permitted, a new certificate reflecting the updated data is issued and the previous version is revoked if necessary.

4.8.4 Notification of new certificate issuance to subscriber

TSA personnel are notified via the secure internal communication channel and the updated certificate is delivered through a trusted path.

4.8.5 Conduct acceptance of modified certificate

Same procedures as in Section 4.4.1 apply. Operational logging and audit trails must document the change.

4.8.6 Publication of the modified certificate by the CA

Published as a new certificate in the public repository. Old versions will be archived indefinitely.

4.8.7 Notification of certificate issuance by the CA to other entities

Same as in previous sections; supervisory body is informed only if required.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

Revocation of a TSA certificate is performed if:

- The private key is suspected or confirmed to be compromised,
- The certificate was issued with incorrect data or violates policy,
- The TSA or Root CA ceases operations or is restructured,
- Regulatory or supervisory directives require such action.

4.9.2 Who can request revocation

Revocation can be initiated by:

- TSA authorized personnel,
- Timestamp Root CA personnel,
- Regulatory/supervisory bodies,
- Internal incident response or security team.

4.9.3 Procedure for revocation request

Revocation requests must be:

- Authenticated via multi-factor procedures (e.g., secure admin access, incident response authorization) or digitally signed by at least 2 authorized personal defined in 4.9.2.,
- Documented in the incident response and CA lifecycle logs,
- Approved by designated security officers.

Once approved, the certificate is added to the current CRL without undue delay.

4.9.4 Revocation request grace period

Requests are acted upon without delay, and in any case, within 6 hours of confirmed compromise or policy violation.

4.9.5 Time within which CA must process the revocation request

The Timestamp Root CA will process confirmed revocation requests within 15 hours and publish the updated CRL within 1 hour thereafter.

4.9.6 Revocation checking requirement for relying parties

Relying parties are required to validate certificate status using:

- CRLs published via HTTP by the CA.

Validation should occur at the time of verifying timestamp signatures to ensure integrity and compliance.

4.9.7 CRL issuance frequency

- CRLs are issued at least every 2 months even if no changes occur,
- In the event of a revocation, a new CRL is issued immediately.

4.9.8 Maximum latency for CRLs

New or updated CRLs are published within 1 hour of generation.

4.9.9 On-line revocation/status checking availability

The Timestamp Root CA does not provide an OCSP service for certificate status. Relying parties must use CRLs as the sole method for certificate status checking.

4.9.10 On-line revocation checking requirements

As OCSP is not supported, applications must be capable of parsing and verifying CRLs published via HTTP.

4.9.11 Other forms of revocation advertisements available

TSA authority publishes information regarding TSA key compromise, revocation and/renewal for its clients and relying parties on its public pages (used for certificate publication).

4.9.12 Special requirements regarding key compromise

In case of key compromise:

- Immediate revocation is mandated,
- Notification must be sent to the supervisory authority within 24 hours,
- All affected systems must switch to a backup or re-keyed certificate,
- A full incident analysis is launched.

4.9.13 Circumstances for suspension

Certificate suspension is not supported. Suspension is not supported due to the critical role of timestamping operations. Certificate validity status is binary (valid/revoked), ensuring unambiguous trust decisions for relying parties.

4.10Certificate Status Services

The Timestamp Root CA provides the following certificate status information services:

- CRL Service: Published at a known, publicly accessible HTTP URL and updated per the schedule in Section 4.9.7. It contains a list of revoked certificates in DER format and is signed by the CA,
- OCSP: Not available.

Relying parties are expected to:

- Retrieve and validate the latest CRL before accepting a TSA certificate as valid,
- Implement automatic CRL refresh mechanisms in their validation tools.

The availability of the CRL service is ensured 24x7 with high availability infrastructure, including redundant web servers and monitored publication jobs.

4.11Timestamp request handling

Incert TSA provides timestamping services through a secure and authenticated API, compliant with the Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) defined in RFC 3161.

Each time-stamp request must include:

- A message imprint, which is a cryptographic hash (e.g., SHA-256) of the data to be timestamped
- An identifier of the hash algorithm used to generate the imprint
- An optional nonce, which enhances security by protecting against replay attacks and is unique to the timestamp request and response objects.

Only authorized and onboarded subscribers may submit timestamp requests. Subscriber credentials are verified at each request, and request formats are validated for correctness and consistency. Invalid or unauthenticated requests are rejected, and the event is logged.

4.12Timestamp Token Generation and Response

Upon receiving a valid and authenticated request, the Incert TSA performs the following operations:

4.12.1 Timestamp Acquisition

The TSA queries its internal clock, which is tightly synchronized with trusted Coordinated Universal Time (UTC(k)) sources to ensure high accuracy. The obtained time is verified to be within acceptable drift parameters (±1 second).

4.12.2 Token Construction

A time-stamp token (TST) is constructed, embedding the following elements:

- The message imprint and its associated hash algorithm
- The nonce (if provided)
- A serial number for audit traceability
- The timestamp in UTC
- Accuracy and ordering indicators

4.12.3 Digital Signature

The TST is signed using the dedicated TSA private key, which resides within a certified Hardware Security Module (HSM). This signature attests to the validity and integrity of the timestamp and all associated metadata.

4.12.4 Response Delivery

The signed TST is returned to the subscriber through the same secure channel used for submission.

Incert ensures low-latency response times and consistent availability of the TSA endpoint, even during periods of high load.

4.13Token validity and certificate revocation

Time-stamp tokens, once issued, are not revocable. They remain valid indefinitely provided that:

- The TSA's signing certificate was valid at the time of issuance
- The cryptographic algorithms used are still considered secure
- The time embedded within the token is proven to have been synchronized to UTC

However, in the event of compromise or expiration of the TSA’s signing certificate, Incert will:

- Immediately revoke the certificate and publish its status through CRLs

- Inform subscribers about the timestamp authority being compromised and revoked, through the repository notifications
- Terminate issuance of new TSTs under the compromised key
- Initiate key rollover following established key lifecycle procedures

Subscribers and Relying Parties are responsible for verifying the validity of the TSA certificate at the time of TST verification.

4.14Service Continuity and Availability

The Incert TSA is architected for high availability and fault tolerance, incorporating:

- Redundant timestamping units
- Automated failover
- 24x7 monitoring

Incert commits to maintaining timestamping service availability as per its Service Level Objectives (SLOs) and contractual agreements with subscribers. Planned downtimes are announced in advance. Unplanned service interruptions are recorded in the audit trail and incident reports, and may trigger incident response procedures.

5 Facility, Management, and Operational Controls

This section outlines the physical, procedural, and personnel security measures implemented to protect the Timestamp Root CA and the TSA infrastructure and operations . These controls are aligned with ETSI EN 319 411-1/2, ETSI EN 319 421, and applicable requirements of the eIDAS Regulation.

5.1 Physical Security

5.1.1 Site Location and Construction

The Timestamp Root CA is hosted in a secure, access-controlled data centre facility designed to meet Tier III or higher standards. The data centre is physically separated from other TSP environments (i.e. dedicated room) and incorporates the following:

- Fire-resistant construction with restricted access zones,
- Dedicated rooms for cryptographic hardware (e.g., Hardware Security Modules - HSMs),

- Multi-layer perimeter security with monitored entry points.

The same datacenter hosts the system related to the TSA but remain online, while the timestamp Root CA is stored offline or semi-offline so that it’s isolated and accessible only by treated personnel under dual control procedures.

5.1.2 Physical Access

Access to Root CA and TSA facilities is strictly limited to authorized personnel and is protected through:

- Biometric access control and smart card authentication,
- 24x7 surveillance (CCTV), with video retention as per datacenter policy,
- Dual-person control (four-eyes principle) for critical areas such as the key management room,
- Visitor access logging, with escorts required at all times.

5.1.3 Power and Air Conditioning

- Redundant power supply (UPS and diesel generators) ensures uninterrupted operations,
- Precision air-conditioning maintains optimal temperature and humidity for cryptographic devices.

5.1.4 Water Exposures

- Facilities are above flood level with moisture detection systems installed,
- Equipment is raised to avoid ground-level water damage.

5.1.5 Fire Prevention and Protection

- Fire detection via smoke and heat sensors,
- Fire suppression via inert gas or clean agent systems that do not damage electronic equipment.

5.1.6 Media Storage

- All backup media and cryptographic tokens are stored in secure, access-controlled safes or cabinets in Incert premises (Office),

5.1.7 Waste Disposal

- Sensitive materials are disposed of via certified shredding and demagnetizing services,
- Electronic storage media is wiped using secure deletion protocols before disposal.

5.1.8 Off-Site Backup

- Off-site backups are encrypted and stored at a location geographically distinct from the primary site,
- Recovery procedures are tested annually.

5.2 Procedural Controls

5.2.1 Trusted Roles

The following roles are defined and require trust designation:

- CA Administrator: Manages CA software, certificate issuance and cryptographic key lifecycle events,
- Security and Audit Manager: Oversees compliance, audit preparation, as well as incident response and log reviews ,
- System Administrator: Maintains supporting systems (OS, DB).

All actions related to CA keys or certificate issuance require dual control and are logged.

5.2.2 Number of Persons Required per Task

- Key generation, backup, or restoration requires at least two persons (dual control),
- System configuration changes require approval and are implemented under supervision,
- Routine operations such as CRL publishing may be handled by one trusted individual with audit trails.

5.2.3 Identification and Authentication for Each Role

- Personnel are authenticated using multi-factor authentication (e.g., smart card + PIN),
- Access to CA systems is governed by role-based access control,
- Authentication credentials are reviewed periodically.

5.2.4 Roles Requiring Separation of Duties

To prevent collusion and mitigate risks:

- The roles of Security Officer and CA Administrator are strictly separated,
- No single individual may hold roles across both operations and audit/compliance.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel assigned to trusted roles must:

- Have relevant experience in cryptography, PKI, or IT security,
- Undergo background verification (criminal record check, employment history),
- Hold appropriate security clearance based on risk classification of their duties.

5.3.2 Background Check Procedures

- Conducted prior to onboarding into trusted roles,
- Includes identity verification, employment and education history, and criminal background screening.

5.3.3 Training Requirements

All personnel are provided training on:

- Security policies and incident response,
- Use of cryptographic devices and key ceremony procedures,
- Compliance with CP/CPS and applicable legal frameworks.

5.3.4 Retraining Frequency and Requirements

- Retraining is conducted at least annually or upon major policy changes,
- Attendance is mandatory and documented.

5.3.5 Job Rotation Frequency and Sequence

Not mandatory but considered for specific roles to reduce operational risk. Cross-training is provided.

5.3.6 Sanctions for Unauthorized Actions

Violations of policy result in:

- Immediate access revocation,
- Disciplinary actions,
- Potential legal proceedings, depending on severity.

5.3.7 Independent Contractor Requirements

Contractors in trusted roles must:

- Sign NDAs and undergo the same vetting as full-time personnel,
- Be supervised and limited in scope of access.

5.3.8 Documentation Supplied to Personnel

All personnel receive:

- The latest CP/CPS,
- Security and operational policy documents,
- Incident handling and business continuity procedures.

6 Technical Security Controls

This section describes the technical mechanisms and procedures used by the Timestamp Root CA and the TSA to protect its cryptographic keys, systems, and data. These controls ensure the confidentiality, integrity, and availability of the Timestamp Root CA services in line with ETSI EN 319 411-1/2 and ETSI EN 319 421..

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

- Timestamp Root CA and TSA key pairs are generated within a FIPS 140-2 Level 3 or Common Criteria EAL4+ certified Hardware Security Module (HSM),
- Generation of Timestamp Root CA key pair is performed in a formal key ceremony, witnessed and recorded, with dual control and multi-person integrity (e.g., at least 2 out of 3 trusted individuals),
- The ceremony follows a documented and pre-approved script that includes contingency handling and post-ceremony verification.

6.1.2 Private Key Delivery to Subscriber

- The Timestamp Root CA does not deliver private keys to any external entity,
- The TSA's certificate will be issued by the Root CA, but the TSA key pair will be generated independently by the TSA operator and the Certificate Signing Request (CSR) will be submitted to the Timestamp Root CA.

6.1.3 Public Key Delivery to Certificate Issuer

As a self-signed CA, this does not apply.

For the TSA, the public key is handled for certificate issuance as part of a formal key ceremony.

6.1.4 CA Public Key Delivery to Relying Parties

The Timestamp Root CA certificate is made publicly available through:

- The CA's website and repository service,
- The EU Trusted List (LOTL/TSL) once the CA is included post-audit,
- In downloadable formats (DER format).

6.1.5 Key Sizes and Algorithms

- The Timestamp Root CA and the TSA uses an ECC P-384 key pair depending on cryptographic policy,
- Signature algorithm: ECDSA with SHA-384, compliant with [SOG-IS] and eIDAS recommendations.

6.1.6 Public Key Parameters Generation and Quality Checking

- Parameters for ECC keys are generated according to recognized standards (e.g., NIST or Brainpool curves),
- The HSM enforces proper parameter selection and integrity checks during key pair generation.

6.1.7 Key Usage Purposes

Timestamp Root CA keys are strictly limited to:

- Certificate signing (keyCertSign),
- CRL signing (cRLSign).

No data encryption or key agreement operations are permitted.

For TSA, the keys can only be used for non-repudiation, with the extended key usage being define as timestamping (i.e. OID: 1.3.6.1.5.5.7.3.8).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

All Root CA and TSA private keys reside in an HSM certified at FIPS 140-2 Level 3 or Common Criteria EAL4+.

The HSM enforces:

- Access control per role,
- Logical and physical tamper resistance,
- Secure key backup and zeroization procedures.

6.2.2 Private Key (m out of n) Multi-Person Control

Critical key management actions (generation, backup, restore) require multi-person control, typically 2-out-of-3 trusted individuals.

6.2.3 Private Key Escrow

Not performed. Root CA private keys are never escrowed under any circumstances.

6.2.4 Private Key Backup

- Keys are backed up in encrypted form and stored in a safe located in an access-controlled secure location, such as Incert Premise (Office),
- Backup media is handled only during a key ceremony and stored in an access-controlled secure location.

6.2.5 Private Key Archival

- Archival of private keys is not practiced for the Root CA,
- Expired Root CA keys are securely destroyed after their operational lifetime.

6.2.6 Private Key Transfer into or From a Cryptographic Module

Keys are generated and stored within the HSM. Transfer outside the HSM is prohibited (except for the encrypted backup which is secure as defined in 6.2.4).

6.2.7 Private Key Storage on Cryptographic Module

- Keys are securely stored in non-exportable format in the HSM,
- Access is controlled via strong authentication and role-based policies.

6.2.8 Method of Activating Private Key

Regarding the Timestamp Root CA:

- Root CA key activation requires dual control using cryptographic tokens and PINs/passwords,
- Activation is temporary and only during certificate issuance or CRL signing sessions.

For the TSA keys, they remain active to be able to handle operations, but their usage is strictly controlled and logged for traceability.

6.2.9 Method of Deactivating Private Key

- Timestamp Root CA Keys are automatically deactivated after operations or upon session timeout,
- The HSM (i.e. for Timestamp Root CA and TSA) auto-locks upon security event.

6.2.10 Method of Destroying Private Key

Keys are zeroized using HSM-native secure deletion processes during retirement or compromise.

6.2.11 Cryptographic Module Rating

As noted, only modules certified to FIPS 140-2 Level 3 or Common Criteria EAL4+ are permitted.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The Timestamp Root CA’s public key and associated certificate are archived for a minimum of 20 years after the expiration or revocation of the Root CA certificate, in accordance with ETSI EN 319 411-1 and legal retention requirements applicable to qualified trust services.

This retention period supports long-term validation (LTV) and ensures that relying parties can verify timestamp tokens even after the CA’s operational lifetime.

6.3.2 Certificate Operational Periods and Key Usage Periods

- Root CA certificate validity: 22 years,
- Root CA key usage: limited to 21 years with 1 year overlap for transition,
- Certificates issued by the Root CA (e.g., TSA certificate) may have a shorter validity period (e.g., 7 years), subject to policy.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

- Activation data (e.g., PINs or passwords for HSM tokens) are randomly generated and distributed securely to trusted role holders,
- Each holder receives only part of the data when required for dual control.

6.4.2 Activation Data Protection

- Physically, stored only on tamper-evident sealed envelopes in locked safes,
- Electronically, stored only in encrypted form within approved password manager,
- Never electronically transmitted or stored in plaintext.

6.4.3 Other Aspects of Activation Data

Activation credentials are rotated periodically or upon role changes.

6.5 Computer Security Controls

- Dedicated, hardened systems are used for CA operations,
- Operating systems are configured following security baselines and vendor best practices,
- CA systems are isolated from general IT networks and internet,
- Only essential services are enabled; all others are disabled or removed.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

- CA software and scripts are developed in-house or obtained from verified vendors,
- Changes are tested in a staging environment and follow change management procedures with rollback plans.

6.6.2 Security Management Controls

- Security events are logged, monitored, and analyzed regularly,
- Vulnerability assessments and penetration tests are conducted at least annually.

6.6.3 Life Cycle Security Controls

- All hardware and software used by the CA are tracked through asset management,
- Decommissioning of systems follows secure erasure and physical destruction protocols.

6.7 Life Cycle Technical Controls

- CA systems operate on segmented, firewalled networks with strict ingress/egress rules,
- Only pre-approved IP ranges and ports are allowed,
- Intrusion Detection and Prevention Systems (IDPS) monitor network traffic.

6.8 Time-Stamping

- A TST is not applicable for the Root CA, as it does not issue timestamp tokens directly. The date/time used at the Timestamp Root CA servers is still in synchronization with the internal trusted NTP servers.
- Time-stamping responsibilities are handled by the TSA, which receives its certificate from the Root CA.

6.8.1 Time Synchronization and Accuracy Assurance

The reliability of timestamping depends on accurate timekeeping. Incert synchronizes its systems with trusted UTC(k) time sources using authenticated Network Time Protocol (NTP) and/or GNSS receivers where required.

- Clocks are monitored continuously to ensure deviation stays within ±1 second of UTC
- Automatic controls are in place to halt TST issuance if synchronization thresholds are breached
- Clock corrections, leap second insertions, and synchronization failures are logged and reviewed

This ensures that every time-stamp token issued is cryptographically verifiable and temporally trustworthy.

6.8.2 Event Logging and Audit Trails

A detailed log is maintained for every significant event within the TSA environment, including:

- All timestamp requests and responses
- System configuration changes
- User access and role assignments
- Key generation, activation, and retirement
- Clock drift incidents and corrections

Logs are:

- Signed to ensure integrity
- Stored in a secure, append-only format
- Archived for a minimum of 7 years
- Reviewed regularly by compliance officers and subject to external audit

Access to logs is strictly controlled and limited to authorized personnel only.

7 Certificate, CRL, and OCSP Profiles

This section defines the technical specifications of certificates issued by the Timestamp Root CA, as well as the structure and content of Certificate Revocation Lists (CRLs). Since the Root CA does not provide an Online Certificate Status Protocol (OCSP) service itself, OCSP profiles are noted as not applicable.

7.1 Certificate Profile

7.1.1 Version Number

Certificates issued by the Timestamp Root CA are X.509 version 3 (v3).

7.1.2 Certificate Extensions

The standard extensions included in the Timestamp Root CA certificate are documented in the HPKI - naming and profile document.

7.1.3 Algorithm and Key Length

The Signature Algorithm, key algorithm and key size are documented in the HPKI - naming and profile document.

7.1.4 Name Forms

The subject Distinguished name is documented in the HPKI - naming and profile document.

7.1.5 Certificate Validity Period

- The Root CA certificate typically has a validity period of 22 years, defined at issuance and based on policy and audit requirements,
- The actual validity is set to ensure that all issued certificates (e.g., TSA certificates) remain valid within the Root CA lifetime.

7.1.6 Certificate Policy Object Identifier (OID)

The certificate will include the CP OID uniquely identifying this CP/CPS document, e.g.: 1.3.171.5.3.2.2.1.0 (illustrative only).

7.1.7 CPS Pointer

The cpsPointer field within the certificate references the URL to the official published CPS document.

7.2 TSA Certificate Profile

Incert TSA uses dedicated X.509 v3 certificates for timestamp signing. These certificates:

- Are issued by a trusted CA within the Incert PKI hierarchy

- Contain the KeyUsage extension with digitalSignature set
- Include the ExtendedKeyUsage extension with timeStamping (OID: 1.3.6.1.5.5.7.3.8)
- Are bound to this CP through the PolicyIdentifier extension (OID: 1.3.171.5.3.2.2.1.0)
- Are valid for a maximum of 7 years and subject to controlled renewal
- Are published in the TSA repository and included in signed responses for validation purposes

The TSA certificate is issued by the Timestamp Root CA, a dedicated, self-signed trust anchor operated by Incert and listed in the EU Trusted List. The certificate chain includes:

- TSA Certificate (leaf, qualified for timestamping use)
- TSA Root CA (self-signed)

This hierarchy ensures direct and verifiable trust in time-stamp tokens through an audited and published root.

TSA certificates are not used for signing documents, authentication, or TLS but only to issue TSTs.

The complete certificate profile is documented in the HPKI - naming and profile document.

7.3 Timestamp Token Structure

All tokens issued by Incert TSA follow the format defined in RFC 3161 and ETSI EN 319 422, and contain:

- A message imprint (i.e., the hash of data being timestamped)
- The hash algorithm used (e.g., SHA-256)
- A unique serial number
- A precise time value in UTC, accurate within ±1 second
- The TSA certificate reference
- Optional nonce (as provided in the request)
- A digital signature produced using the TSA private key

Tokens are returned in DER-encoded ASN.1 format and are designed to support long-term validation (LTV) through cryptographic timestamping chains and archived certificates.

Tokens may be embedded into signed documents, attached to logs, or used independently as standalone time proofs.

7.4 CRL Profile

7.4.1 Version

All CRLs are X.509 version 2 (v2).

7.4.2 CRL Extensions

The standard CRL extensions included in the CRL issued by the Timestamp Root CA certificate are documented in the HPKI - naming and profile document.

7.4.3 CRL Issuance Frequency

- The Root CA issues CRLs at least every 2 months, or immediately upon revocation of a TSA certificate,
- A “nextUpdate” field is used to define the expected next CRL publication date.

7.4.4 CRL Distribution Point (CDP)

CRLs are made publicly available through:

- HTTP URLs hosted on the CA’s public repository,
- Accessible locations as defined in the CDP extension of issued certificates,
- Optionally via publication to trusted lists or state registries, as required.

7.5 OCSP Profile

- Not applicable,
- .The Timestamp Root CA does not provide OCSP responses. Relying parties must use the CRL distribution points specified in issued certificates. This approach complies with ETSI EN 319 411-1 where CRLs are recognized as a valid revocation status mechanism.

8 Compliance Audit and Other Assessments

This section describes the policies and procedures related to the compliance assessments and audits performed to ensure the Timestamp Root CA operates in accordance with applicable standards, regulatory requirements, and the practices set forth in this CP/CPS.

8.1 Frequency or Circumstances of Assessment

The Timestamp Root CA is subject to regular compliance audits to ensure conformance with:

- eIDAS Regulation (EU) No 910/2014, including requirements for Qualified Trust Service Providers (QTSPs) and Qualified Trust Services (QTS),
- Applicable ETSI standards, particularly EN 319 401, EN 319 411-1, and EN 319 411-2, as relevant to issuing qualified certificates,
- The practices stated in this CP/CPS and any internal operational policies.

A full conformity assessment is performed prior to initial inclusion of the Root CA certificate in the EU Trust List.

Following a positive initial conformity assessment, the supervisory authority validates the audit report and facilitates the inclusion of the Root CA in the EU Trusted List (LOTL/TSL).

Surveillance (follow-up) audits are carried out annually or more frequently if required by the supervisory body or triggered by changes in infrastructure, incidents, or findings.

Internal audits are also carried out annually or more frequently if triggered by changes in infrastructure, incidents, or findings.

8.2 Identity/Qualifications of Assessor

Assessments are conducted by a qualified, independent Conformity Assessment Body (CAB) that:

- Is accredited under a national accreditation scheme aligned with Regulation (EC) No 765/2008,
- Has demonstrable competence in evaluating trust service providers and public key infrastructures.

The CAB must be recognized by the national supervisory body responsible for trust services under the eIDAS framework.

8.3 Assessor's Relationship to Assessed Entity

- The CAB operates independently and maintains an arm’s length relationship with the CA operator,
- The CAB has no financial or operational ties that could compromise the impartiality or objectivity of the assessment,
- The CA must disclose any potential conflict of interest to the supervisory body in advance.

8.4 Topics Covered by Assessment

The compliance audit covers, but is not limited to, the following areas:

- Governance and operational management of the Timestamp Root CA,
- Physical and logical security controls of key material and infrastructure,
- Certificate lifecycle management (including key generation, issuance, and revocation),
- Conformance of CA certificate profiles to applicable technical standards,
- CRL generation, distribution, and retention,
- Personnel security and role-based access controls,
- Documentation, including CP/CPS compliance,
- Incident handling and business continuity measures,
- Internal audit procedures and quality controls.

8.5 Actions Taken as a Result of Deficiency

Any non-conformities or findings identified during the audit are addressed through:

- A documented remediation plan with clear responsibilities and timelines,
- Carrying out in-depth root cause analysis,
- Re-assessment or verification by the CAB if required.

Serious deficiencies that could impact trust in the Root CA services may lead to:

- Temporary suspension or revocation of CA operations,
- Withdrawal of the CA certificate from the EU Trust List by the supervisory body.

The CA must notify affected relying parties and the supervisory body where necessary.

8.6 Communication of Results

- Upon successful audit, the conformity assessment report is submitted to the national supervisory body for validation,
- If validated, the supervisory body facilitates the inclusion of the Root CA certificate in the EU Trust List,
- A summary of the audit results may be published in line with applicable transparency requirements,

- Internal audit reports and sensitive information remain confidential unless disclosure is mandated by regulation,

9 Other Business and Legal Matters

This section outlines the legal, financial, and administrative matters related to the operation of the Timestamp Root CA, including liability, fees, intellectual property rights, privacy, and dispute resolution mechanisms.

9.1 Fees

The CA does not charge relying parties for accessing publicly available certificates, CRLs, or the CP/CPS.

Fees may be charged to subordinate entities (e.g., TSA operators) for:

- Certificate issuance and lifecycle services,
- Audit or re-audit services, if triggered by client-side non-compliance.

Any such fees, if applicable, are documented in the contractual agreements with the affected parties.

9.2 Financial Responsibility

The CA maintains appropriate financial resources and insurance coverage, as required under the applicable national laws for Qualified Trust Service Providers.

This includes coverage for:

- Potential liabilities from CA service failures,
- Business continuity and disaster recovery operations.

The CA performs risk assessments regularly to ensure adequacy of coverage.

9.3 Confidentiality of Business Information

Information marked as confidential and not publicly disclosed through CP/CPS, CRLs, or certificate repositories is protected in accordance with:

- The applicable national legislation,
- The CA’s internal security and confidentiality policies.

Access to sensitive information is limited to authorized personnel and is protected using technical and procedural safeguards.

9.4 Privacy of Personal Information

The CA complies with the General Data Protection Regulation (GDPR) (EU Regulation 2016/679).

Personal data collected in the course of certificate issuance (e.g., for identity verification) is:

- Used strictly for the purposes of trust service provision,
- Processed lawfully, fairly, and transparently,
- Retained only for as long as necessary for legal or operational purposes.

Data subjects (TSAs) have the right to access, rectify, and request erasure of their personal data, subject to legal and contractual obligations.

9.5 Intellectual Property Rights

All documentation, including this CP/CPS, as well as certificate profiles and repositories, are the intellectual property of the CA (INCERT), unless otherwise stated.

Use of Root CA certificates and associated materials by relying parties is permitted under the terms defined in this CP/CPS, solely for the purpose of verifying qualified electronic timestamps.

9.6 Representations and Warranties

The CA represents and warrants that:

- It operates in conformance with the applicable legal and regulatory frameworks, including eIDAS and ETSI standards,
- Certificates are issued only after proper identity verification and key management procedures,
- Certificate data and revocation status information are accurate at the time of issuance and publication.

Relying parties are expected to:

- Validate the certificate status using CRLs or other mechanisms prior to trust decisions,
- Use certificates only for their intended purposes.

9.7 Disclaimers of Warranties

- Except as explicitly stated in this CP/CPS, the CA disclaims all other warranties, including implied warranties of merchantability or fitness for a particular purpose,

- The CA does not warrant that use of certificates will be uninterrupted or error free, or that relying parties will not experience damage or loss.

9.8 Limitations of Liability

The CA’s liability is limited to damages directly attributable to negligent failure to comply with this CP/CPS or applicable laws.

The CA shall not be liable for:

- Indirect or consequential damages,
- Loss of profits, business, or data due to reliance on expired, revoked, or misused certificates.

Maximum liability amounts, if applicable, are stated in contractual agreements or published terms of service.

9.9 Indemnities

Certificate subscribers and relying parties shall indemnify and hold harmless the CA for:

- Any misuse of certificates,
- Non-compliance with the terms of this CP/CPS,
- Breach of contractual or regulatory obligations.

9.10Term and Termination

This CP/CPS is effective upon publication and remains valid until replaced by a newer version or until termination of the CA services.

The CA may terminate its services under conditions such as:

- Voluntary shutdown,
- Revocation of accreditation,
- Regulatory order or legal judgment.

In such cases, appropriate steps will be taken to:

- Notify affected parties,
- Revoke issued certificates,
- Still maintain repository access for a defined archival period.

9.11 Individual Notices and Communications with Participants

Official communications are conducted through:

- Email addresses listed in this CP/CPS,
- CA’s official website or secure repositories.

Participants may be contacted using the information provided during registration or contractual agreement.

9.12 Amendments

This CP/CPS is reviewed at least annually or more frequently in case of:

- Regulatory changes,
- Major operational or technical changes.

Changes are made following an internal review and stakeholder consultation. Each version is assigned a unique version number and effective date.

9.13 Dispute Resolution Provisions

Any disputes between the CA and its subscribers, relying parties, or auditors shall be resolved:

- In accordance with applicable national law,
- Through arbitration or mediation where required or agreed contractually.

The CA designates the courts of the Grand-Duchy of Luxembourg as the competent jurisdiction in the event of disputes between the parties

9.14 Governing Law

This CP/CPS and all CA-related operations are governed by the laws of Grand Duchy of Luxembourg.

9.15 Compliance with Applicable Law

The CA ensures full compliance with:

- eIDAS Regulation,
- GDPR,
- National regulations for qualified trust service providers and PKIs.

9.16Miscellaneous Provisions

- If any provision of this CP/CPS is found to be unenforceable, the remaining provisions shall continue in full force,
- Headings are for reference only and do not affect the interpretation of the content.

9.17Other Provisions

There are no additional provisions not covered in the sections above unless formally communicated and published by the CA.

10GLOSSARY AND REFERENCE DOCUMENTS

10.1Definitions

Term	Definition
CA	Certification Authority – An entity responsible for issuing, managing, and revoking digital certificates.
CP	Certificate Policy – A high-level set of rules indicating the applicability of a certificate to a particular community or class of application.
CPS	Certification Practice Statement – A detailed description of the practices followed by a CA in managing certificates.
CRL	Certificate Revocation List – A signed list issued by a CA that identifies revoked but not yet expired certificates.
eIDAS	Electronic Identification, Authentication and Trust Services – EU regulation establishing a framework for electronic trust services.
QTSP	Qualified Trust Service Provider – A trust service provider that meets the requirements under eIDAS and is included in the EU Trusted List.
RA	Registration Authority – An entity that acts on behalf of a CA to perform identification and authentication of certificate subjects.
TSA	Time-Stamping Authority – An entity that issues time-stamps conforming to a defined policy.
TSP	Trust Service Provider – An entity providing electronic trust services, such as certificate issuance or timestamping.
OCSP	Online Certificate Status Protocol – A method for checking the revocation status of a certificate in real-time.
TST	Timestamp Token – A trusted timestamp token digitally signed by the Timestamp Authority Certificate's corresponding private key.

10.2 Acronyms

- **API** – Application Programming Interface
- **CAB** – Conformity Assessment Body
- **CP** – Certificate Policy
- **CPS** – Certification Practice Statement
- **DR** – Disaster Recovery
- **HSM** – Hardware Security Module
- **ISMS** – Information Security Management System
- **LTV** – Long-Term Validation
- **NTP** – Network Time Protocol
- **PKI** – Public Key Infrastructure
- **RPO** – Recovery Point Objective
- **RTO** – Recovery Time Objective
- **TSA** – Timestamp Authority

10.3 Reference Documents

Reference	**Document Name**
ETSI EN 319 421	Policy and security requirements for Trust Service Providers providing time-stamping
ETSI EN 319 422	Time-stamping protocol and time-stamp token profiles
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol
ETSI EN 319 401	General policy requirements for trust service providers
FIPS PUB 140-3	U.S. Federal standard for cryptographic module security
ISO/IEC 27001	Information Security Management standard
ISO/IEC 15408	Common Criteria for IT Security Evaluation

Reference	Document Name
Regulation (EU) 910/2014	eIDAS Regulation on trust services and digital identity