



HOPAE S.A. — INFORMATION SECURITY & TRUST DOCUMENTATION

# Hopae Timestamping Service Certificate Policy and Certification Practice Statement

H\_P\_TSPS · Version 1.2 · Approved

|                |                                                                                                        |
|----------------|--------------------------------------------------------------------------------------------------------|
| DOCUMENT ID    | H_P_TSPS — Hopae Timestamping Service Certificate Policy and Certification Practice Statement (CP/CPS) |
| VERSION        | 1.2                                                                                                    |
| STATUS         | Approved v1.2                                                                                          |
| CLASSIFICATION | Public                                                                                                 |
| EFFECTIVE DATE | 03/09/2026                                                                                             |
| LAST UPDATED   | 03/09/2026                                                                                             |
| POLICY OWNER   | Junmin Kim (Eric Kim) (Head of Trust & Security Officer)                                               |
| APPROVED BY    | Jaehoon Shim (Ace Shim), CEO                                                                           |
| ENTITY SCOPE   | Hopae S.A.; group applicability per GRC Register Scope                                                 |

## Contents

|                                                                    |    |
|--------------------------------------------------------------------|----|
| Document Control.....                                              | 5  |
| Standards and Regulatory Coverage.....                             | 5  |
| 1. INTRODUCTION.....                                               | 5  |
| 1.1 Overview.....                                                  | 6  |
| 1.2 Document Name and Identification.....                          | 7  |
| 1.3 PKI Participants.....                                          | 7  |
| 1.4 Certificate Usage.....                                         | 9  |
| 1.5 Policy Administration.....                                     | 10 |
| 1.6 Definitions and Acronyms.....                                  | 15 |
| 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....                | 15 |
| 2.1 Repository Access.....                                         | 15 |
| 2.2 Publication of Certification Information.....                  | 16 |
| 2.3 Time or Frequency of Publication.....                          | 16 |
| 2.4 Access Controls.....                                           | 17 |
| 3. IDENTIFICATION AND AUTHENTICATION.....                          | 17 |
| 3.1 Naming.....                                                    | 17 |
| 3.2 Initial Identity Validation.....                               | 18 |
| 3.3 Identification and Authentication for Re-Key Requests.....     | 19 |
| 3.4 Identification and Authentication for Revocation Requests..... | 19 |
| 4. CERTIFICATE LIFE CYCLE AND TSA OPERATIONAL REQUIREMENTS.....    | 20 |
| 4.1 Certificate Application.....                                   | 20 |
| 4.2 Certificate Application Processing.....                        | 21 |
| 4.3 Certificate Issuance.....                                      | 21 |
| 4.4 Certificate Acceptance.....                                    | 21 |
| 4.5 Key Pair and Certificate Usage.....                            | 22 |
| 4.6 Certificate Renewal.....                                       | 23 |
| 4.7 Certificate Re-Key.....                                        | 23 |
| 4.8 Certificate Modification.....                                  | 24 |

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| 4.9 Certificate Revocation and Suspension.....                                | 25 |
| 4.10 Certificate Status Services.....                                         | 26 |
| 4.11 Timestamp Request Handling.....                                          | 27 |
| 4.12 Timestamp Token Generation and Response.....                             | 27 |
| 4.13 Token Validity and Certificate Revocation.....                           | 28 |
| 4.14 Service Continuity and Availability.....                                 | 28 |
| 4.15 Notification of Changes in Trust Service Provision.....                  | 28 |
| 5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS.....                        | 29 |
| 5.1 Physical Security.....                                                    | 30 |
| 5.2 Procedural Controls.....                                                  | 31 |
| 5.3 Personnel Controls.....                                                   | 32 |
| 6. TECHNICAL SECURITY CONTROLS.....                                           | 34 |
| 6.1 Key Pair Generation and Installation.....                                 | 34 |
| 6.2 Private Key Protection and Cryptographic Module Engineering Controls..... | 35 |
| 6.3 Other Aspects of Key Pair Management.....                                 | 37 |
| 6.4 Activation Data.....                                                      | 37 |
| 6.5 Computer Security Controls.....                                           | 37 |
| 6.6 Life Cycle Technical Controls.....                                        | 38 |
| 6.7 Network Security Controls.....                                            | 38 |
| 6.8 Time-Stamping.....                                                        | 38 |
| 7. CERTIFICATE, CRL, AND OCSP PROFILES.....                                   | 39 |
| 7.1 Certificate Profile.....                                                  | 39 |
| 7.2 TSA Certificate Profile.....                                              | 40 |
| 7.3 Timestamp Token Structure.....                                            | 40 |
| 7.4 CRL Profile.....                                                          | 41 |
| 7.5 OCSP Profile.....                                                         | 41 |
| 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....                                | 41 |
| 8.1 Frequency or Circumstances of Assessment.....                             | 41 |
| 8.2 Identity/Qualifications of Assessor.....                                  | 42 |
| 8.3 Assessor's Relationship to Assessed Entity.....                           | 42 |

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| 8.4 Topics Covered by Assessment.....                                         | 42 |
| 8.5 Actions Taken as a Result of Deficiency.....                              | 42 |
| 8.6 Communication of Results.....                                             | 43 |
| 9. OTHER BUSINESS AND LEGAL MATTERS.....                                      | 43 |
| 9.1 Fees.....                                                                 | 43 |
| 9.2 Financial Responsibility.....                                             | 43 |
| 9.3 Confidentiality of Business Information.....                              | 44 |
| 9.4 Privacy of Personal Information.....                                      | 44 |
| 9.5 Intellectual Property Rights.....                                         | 44 |
| 9.6 Representations and Warranties.....                                       | 45 |
| 9.7 Disclaimers of Warranties.....                                            | 45 |
| 9.8 Limitations of Liability.....                                             | 45 |
| 9.9 Indemnities.....                                                          | 46 |
| 9.10 Term and Termination.....                                                | 46 |
| 9.11 Individual Notices and Communications with Participants.....             | 47 |
| 9.12 Amendments.....                                                          | 47 |
| 9.13 Dispute Resolution Provisions.....                                       | 47 |
| 9.14 Governing Law.....                                                       | 48 |
| 9.15 Compliance with Applicable Law.....                                      | 48 |
| 9.16 Miscellaneous Provisions.....                                            | 48 |
| 9.17 Other Provisions.....                                                    | 48 |
| 9.18 ISO/IEC 27701 Privacy Information Management System (PIMS) Addendum..... | 48 |
| 10. GLOSSARY AND REFERENCE DOCUMENTS.....                                     | 49 |
| 10.1 Definitions.....                                                         | 49 |
| 10.2 Acronyms.....                                                            | 49 |
| 10.3 Reference Documents.....                                                 | 50 |
| Version History.....                                                          | 50 |

# Document Control

|                       |                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------|
| <b>Document ID</b>    | H_P_TSPS — Hopae Timestamping Service Certificate Policy and Certification Practice Statement (CP/CPS) |
| <b>Policy Owner</b>   | Junmin Kim (Eric Kim) (Head of Trust & Security Officer)                                               |
| <b>Approved By</b>    | Jaehoon Shim (Ace Shim), CEO                                                                           |
| <b>Status</b>         | Approved v1.2                                                                                          |
| <b>Effective Date</b> | 03/09/2026                                                                                             |
| <b>Last Updated</b>   | 03/09/2026                                                                                             |
| <b>Classification</b> | Public                                                                                                 |
| <b>Entity Scope</b>   | Hopae S.A.; group applicability per GRC Register Scope                                                 |

*In small organizations where resources are limited, policy ownership and approval are separated at the executive level. The CEO of Hopae S.A. retains ultimate approval authority.*

Hopae S.A., 20 Rue des Peupliers, 2328 Hamm, Luxembourg

## Standards and Regulatory Coverage

### eIDAS Regulation

- Regulation (EU) No 910/2014, Article 42 (Qualified Electronic Time Stamps)
- Regulation (EU) No 910/2014, Article 24 (Requirements for QTSPs)

### ETSI Standards

- ETSI EN 319 401 — General Policy Requirements for Trust Service Providers
- ETSI EN 319 421 — Policy and Security Requirements for TSPs issuing Time-Stamps
- ETSI EN 319 411-1 — Policy requirements for TSPs issuing certificates
- ETSI EN 319 422 — Time-stamping protocol and time-stamp token profiles

### ISO/IEC Standards

- ISO/IEC 27001:2022 — Information Security Management Systems
- ISO/IEC 27701:2019 — Privacy Information Management

### SOC 2 Trust Services Criteria

- Security, Availability, Processing Integrity

## 1. INTRODUCTION

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which this Certificate Policy (CP) and Certification Practice Statement (CPS) is targeted.

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

## 1.1 Overview

Hopae S.A. (hereinafter “Hopae”) is a global digital identity verification company providing electronic identification (eID) verification services across 190+ countries. Hopae operates the “Hopae Timestamping Service” as a Qualified Trust Service Provider (QTSP) under Regulation (EU) No 910/2014 (eIDAS).

This document constitutes both the Certificate Policy (CP) and Certification Practice Statement (CPS) for the Hopae Timestamping Service. The service provides Qualified Electronic Timestamps in accordance with Article 42 of the eIDAS Regulation and applicable ETSI standards.

### 1.1.1 Delegation Model

Hopae operates its timestamping service under a delegation model with INCERT GIE (hereinafter “INCERT”), a Qualified Trust Service Provider established in Luxembourg. INCERT GIE was founded in 2012 by the State of Luxembourg and the Luxembourg Chamber of Commerce, and has maintained ISO/IEC 27001 certification since 2025.

Under this delegation model:

- INCERT operates the Timestamp Root Certification Authority and issues Timestamping Authority (TSA) certificates
- INCERT operates the cryptographic infrastructure including Hardware Security Modules (HSMs) for TSA key generation and storage
- INCERT performs TSA cryptographic operations (timestamp token signing) on behalf of Hopae
- Hopae retains full legal and regulatory responsibility as the QTSP
- Hopae maintains policy ownership, governance, and liability for the timestamping service
- Hopae is the audit subject for QTSP conformity assessment
- INCERT is subject to separate audits for its infrastructure operations

This combined CP/CPS document is designed to meet the requirements of:

- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers)
- ETSI EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Time- Stamps)
- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates), where applicable to TSA certificates

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

The TSA certificate issued under this Timestamp Root Certification Authority 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 Certification Authority in the EU Trusted List.

The timestamp tokens issued under this policy are intended to be used for long-term validation and legal acceptance of signed data, meeting the requirements for Qualified Electronic Timestamps under the eIDAS Regulation.

### 1.1.2 Policy Object Identifier (OID)

The following OID identifies the time-stamp policy under which the Hopae Timestamping Service operates: 1.3.171.7.1.1.1. This policy OID is allocated under the Hopae S.A. OID arc 1.3.171.7 (registered via ILNAS, Luxembourg) and is status-neutral: it remains unchanged before and after inclusion of the service in the EU Trusted List.

The Hopae OID arc 1.3.171.7 and the time-stamp policy OID 1.3.171.7.1.1.1 are managed in accordance with the OID Management Policy and Procedure (H\_I\_OID-MANAGEMENT-POLICY). Allocation, lifecycle management, and external registration procedures are documented therein.

The OID is embedded in the certificatePolicies extension of every TSA certificate issued under this policy. Verification of correct OID embedding is performed by a Hopae witness during each Key Ceremony, per the INCERT Outsourcing Agreement Article 9.

### 1.1.3 NIS2 Directive Compliance

In accordance with Directive (EU) 2022/2555 (NIS2), Hopae S.A. as a qualified trust service provider is classified as an essential entity. This CP/CPS incorporates NIS2 requirements including cybersecurity risk management measures (Article 21), incident notification obligations (Article 23), and supply chain security considerations. NIS2 compliance is coordinated with the existing eIDAS framework and Luxembourg national transposition measures.

## 1.2 Document Name and Identification

| Attribute     | Value                                                                              |
|---------------|------------------------------------------------------------------------------------|
| Document Name | Hopae Timestamping Service Certificate Policy and Certification Practice Statement |
| OID           | 1.3.171.7.1.1.1 (time-stamp policy; Hopae arc: 1.3.171.7)                          |
| BTSP OID      | 0.4.0.2023.1.1 (ETSI Best Practices Time-Stamping Policy)                          |
| Version       | 1.2                                                                                |
| Status        | Approved (03/09/2026)                                                              |
| Date of Issue | Upon approval                                                                      |

The BTSP policy OID 0.4.0.2023.1.1, as defined in ETSI EN 319 421, indicates that timestamp tokens issued under this policy conform to the requirements for best practices time-stamping as specified by ETSI. It is referenced alongside the Hopae time-stamp policy OID 1.3.171.7.1.1.1 identified in Section 1.1.2.

## 1.3 PKI Participants

### 1.3.1 Qualified Trust Service Provider (QTSP)

Hopae S.A. acts as the Qualified Trust Service Provider for the Hopae Timestamping Service under eIDAS. Hopae is responsible for:

- Overall governance and policy management of the timestamping service
- Legal and regulatory compliance as the QTSP
- Service delivery and subscriber relationship management
- Incident response and notification to supervisory authorities
- Termination planning and service continuity

- Audit responsibility and conformity assessment
- Third-party oversight of INCERT operations

INCERT GIE acts as the technical service provider responsible for:

- Operating the Timestamp Root Certification Authority
- Issuing TSA certificates under the Timestamp Root Certification Authority
- Operating Hardware Security Modules (HSMs) for TSA key management
- Performing TSA cryptographic operations (timestamp token signing)
- Maintaining time synchronization infrastructure synchronized with trusted UTC(k) sources
- Publishing Certificate Revocation Lists (CRLs) for the Timestamp Root Certification Authority
- Maintaining physical security controls for cryptographic infrastructure

INCERT maintains its own CP/CPS for the Timestamp Root Certification Authority (“INCERT Timestamp Root CA and TSA Certificate Policy and Certification Practice Statement”), which governs the technical operations delegated to INCERT.

The Timestamp Root Certification Authority operated by INCERT:

- 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

**Critical Note:** Hopae does not operate a Root Certification Authority, does not issue certificates, and does not operate HSMs directly. All such operations are delegated to INCERT while Hopae retains full regulatory responsibility.

### *1.3.2 Registration Authorities*

Not Applicable. Hopae does not operate a Registration Authority. The timestamping service does not involve subscriber certificate issuance to end users. TSA certificate issuance is handled internally by INCERT under strict procedural and personnel controls. The Timestamp Root Certification Authority performs Registration Authority functions internally.

### *1.3.3 Subscribers*

The Hopae Timestamping Service is provided exclusively to business subscribers (legal entities). Natural persons are not eligible for direct subscription.

Subscribers must:

- Be a legal entity duly registered in their jurisdiction of incorporation
- Execute a Subscriber Agreement incorporating the Terms and Conditions (see Section 9.6.1)
- Complete the onboarding and identity validation process described in Section 3.2
- Authenticate via API credentials issued during onboarding

This service operates as a public qualified trust service available to authorized business subscribers who have completed the contractual onboarding process.

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

### 1.3.4 Relying Parties

Relying Parties are individuals or systems that rely on the cryptographic and temporal validity of timestamp tokens issued by the Hopae Timestamping Service. They may include:

- Industry sector regulators
- Legal professionals and courts
- System integrators and software vendors
- End users verifying document authenticity and timing
- Government agencies requiring temporal evidence
- Archival systems requiring long-term validation

Relying Parties are expected to:

- Validate the certificate status using CRLs before accepting a TSA certificate as valid
- Implement automatic CRL refresh mechanisms in their validation tools
- Use timestamp tokens only within the scope defined in this CP/CPS

### 1.3.5 Other Participants

Other participants in the trust framework include:

- **Supervisory Bodies:** The Luxembourg supervisory authority (ILNAS — Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services) responsible for oversight of Qualified Trust Service Providers
- **Conformity Assessment Bodies:** Accredited auditors performing QTSP conformity assessments under Regulation (EC) No 765/2008
- **INCERT GIE:** Technical service provider for cryptographic operations, operating under separate audit and compliance requirements

## 1.4 Certificate Usage

This CP/CPS applies to the Hopae Timestamping Service. The TSA certificates issued by INCERT's Timestamp Root Certification Authority:

- Are used exclusively for signing timestamp tokens issued under RFC 3161
- Must not be used for signing user documents, email protection, client/server authentication, or code signing
- Are issued and maintained within HSMs operated by INCERT
- Contain the Extended Key Usage extension with timeStamping (OID 1.3.6.1.5.5.7.3.8)
- Contain the Key Usage extension with digitalSignature set

The Timestamp Root Certification Authority certificate:

- May only be used to issue TSA certificates for qualified timestamp token generation
- Must not be used for signing user documents, email protection, client/server authentication, or code signing
- Is maintained within offline HSMs operated by INCERT

Hopae does not issue any certificates directly. Certificate issuance for the TSA is performed by INCERT.

## 1.5 Policy Administration

### 1.5.1 Organization Administering the Document

This CP/CPS and the documents referenced herein are maintained and administered by Hopae S.A., which can be contacted at:

Hopae S.A. 20 Rue des Peupliers 2328 Hamm Grand-Duchy of Luxembourg

Email: [trust@hopae.com](mailto:trust@hopae.com) Website: <https://www.hopae.com>

### 1.5.2 Contact Person

Questions regarding this CP/CPS shall be directed to:

Head of Trust Hopae S.A. 20 Rue des Peupliers 2328 Hamm Grand-Duchy of Luxembourg

Email: [trust@hopae.com](mailto:trust@hopae.com) Tel: +82 10 8427 1117

### 1.5.3 Person Determining CP and CPS Suitability for the Policy

The ISMS Governance Council of Hopae approves this CP/CPS and any subordinated practice statements. The Council is chaired by the Chief Executive Officer (CEO) and includes the Head of Trust & Security Officer and Data Protection Officer.

### 1.5.4 CP and CPS Approval Procedures

Applicable requirement [ETSI EN 319 401, REQ-6.1-06]: “The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP’s practice statement.”

The ISMS Governance Council is the management body with overall responsibility for the Hopae Timestamping Service and holds final authority for approving this CP/CPS. The Council is chaired by the Chief Executive Officer (CEO) and includes the Head of Trust & Security Officer and the Data Protection Officer (see Section 1.5.3). The composition and responsibilities of the Council are defined in 03-ISMS Roles, Responsibilities, and Authorities.

The ISMS Governance Council reviews any modifications, additions, or deletions to this CP/CPS and determines whether such changes are acceptable. At their sole discretion, they must approve or reject any proposed changes.

The set of policies and practices described in this CP/CPS shall be approved by management, published, and communicated to employees and external parties as relevant, in accordance with ETSI EN 319 401 REQ-6.1-02.

Approval authority: The ISMS Governance Council, with the Chief Executive Officer (CEO) holding final approval authority.

Publication procedure: Upon approval, the revised CP/CPS shall be immediately published at <https://trust.hopae.com/> and communicated to:

- All Hopae personnel via Vanta notification
- Subscribers via email notification to registered contact
- The Supervisory Authority (ILNAS) where changes are material
- The Conformity Assessment Body at the next scheduled audit or immediately if changes affect conformity

All CP/CPS versions are archived and previous versions remain accessible for reference.

Applicable requirement [ETSI EN 319 401, REQ-6.1-07]: “The TSP’s management shall implement the practices.”

The Head of Trust & Security Officer is responsible for implementing the approved practices and ensuring that the practices described in this CP/CPS are carried out in accordance with the approved policies. Implementation responsibilities are distributed across the Security Team, Operations Team, Research Team, and Engineering Team as defined in 03-ISMS Roles, Responsibilities, and Authorities.

Changes affecting the trust service require:

- Coordination with INCERT GIE for technical implications
- Risk assessment in accordance with Hopae’s Risk Management Policy
- Notification to the supervisory authority where required by regulation
- Publication of updated documents in the repository

### **Review Process**

Applicable requirement [ETSI EN 319 401, REQ-6.1-08]: “The TSP shall define a review process for the practices including responsibilities for maintaining the TSP’s practice statement.”

Hopae defines a review process for the practices described in this CP/CPS, including responsibilities for maintaining this practice statement.

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

- Regulatory changes affecting the trust service
- Major operational or technical changes
- Findings from audits or incidents
- Changes to the delegation arrangement with INCERT GIE

The Head of Trust & Security Officer is responsible for preparing revisions. The ISMS Governance Council is the final approving authority. Version control, review cycles, and release procedures are governed by 05-ISMS Procedure for the Control of Documented Information.

A change is considered significant where it may impact trust, security objectives, certificate profiles, cryptographic algorithms, delegation arrangements, or compliance with applicable ETSI standards or eIDAS requirements (see also Section 9.12 Amendments).

### **Notification of Changes**

Applicable requirement [ETSI EN 319 401, REQ-6.1-09X]: “The TSP shall notify notice of changes it intends to make in its practice statement.”

Hopae shall give notice of changes it intends to make in this practice statement.

For significant changes, Hopae shall:

- Notify the supervisory authority (ILNAS) in advance of the intended change, where required by regulation
- Communicate the change to subscribers and relying parties through the public repository and, where appropriate, by direct notification
- Coordinate with INCERT GIE where the change affects technical or cryptographic components

Non-material editorial corrections may be published without advance notice.

The communication procedures, including recipients, timing, and mechanisms, are governed by 06-ISMS Information Security Communication Plan.

Changes to the information security policy shall also be communicated to relevant external parties per REQ-6.3-02:

- Subscribers: via email notification
- Relying parties: via publication at [trust.hopae.com](https://trust.hopae.com)
- ILNAS: via official correspondence where changes are material
- CAB: at next scheduled assessment or immediately if material
- INCERT GIE: via written notice per Outsourcing Agreement

### **Post-Approval Publication**

Applicable requirement [ETSI EN 319 401, REQ-6.1-10]: “The TSP shall, following approval as in REQ-6.1-06 above, make the revised TSP’s practice statement immediately available as required under REQ-6.1-05 above.”

Following approval by the ISMS Governance Council, Hopae shall make the revised practice statement immediately available to subscribers and relying parties.

Applicable requirement [ETSI EN 319 401, REQ-6.1-05X]: “The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the service policy.”

This CP/CPS, service terms and conditions, and related documentation are published in Hopae’s public repository at <https://trust.hopae.com/> (see Section 2.1). The publication frequency is governed by Section 2.3: publication occurs upon initial approval and upon each substantive revision.

### **1.5.5 Conformance with ETSI Standards**

This CP/CPS is designed to meet the requirements of:

- ETSI EN 319 421 — Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 401 — General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 — Policy and security requirements for Trust Service Providers issuing certificates (applicable to TSA certificates issued by INCERT)

The ETSI requirement texts reproduced in this section are based on the versions referenced in Section 10.3 (Reference Documents). Where ETSI standards are revised, this section shall be reviewed and updated to reflect the applicable version.

### **Service Scope**

Applicable requirement [ETSI EN 319 421, OVR-5.3-01]: “This policy may be used for public time-stamping services or time-stamping services used within a closed community.”

This policy is used for a public time-stamping service. The Hopae Timestamping Service is not restricted to a closed community. Subscribers and relying parties are defined in Sections 1.3.3 and 1.3.4.

### **Risk Assessment [ETSI EN 319 401, clause 5]**

Applicable requirement [ETSI EN 319 421, OVR-6.1-01]: “The requirements identified in ETSI EN 319 401, clause 5 shall apply.”

The requirements identified in ETSI EN 319 401, clause 5 apply to the Hopae Timestamping Service. Hopae fulfils these requirements as follows:

REQ-5-01: “The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.”

Hopae carries out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues. The risk assessment methodology, scope, and criteria are documented in 04-ISMS Risk Assessment and Risk Treatment Process. Risk assessments are performed at least annually, or upon material change, including changes to the delegation arrangement with INCERT GIE, relevant legislation, or significant external factors.

REQ-5-02: “The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.”

Hopae selects appropriate risk treatment measures taking account of the risk assessment results. The risk treatment measures ensure that the level of security is commensurate to the degree of risk. Selected controls and their justifications are documented in 11-ISMS Statement of Applicability.

NOTE: See ISO/IEC 27005:2022 for guidance on information security risk management as part of an information security management system.

REQ-5-03: “The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).”

Hopae determines all security requirements and operational procedures necessary to implement the chosen risk treatment measures. These are documented in:

- 02-ISMS Information Security Management System Policy (overarching security requirements)
- This CP/CPS (operational procedures for the timestamping service)
- The supporting information security policies enumerated in 00-ISMS Master List of Documents

REQ-5-04: “The risk assessment shall be regularly reviewed and revised.”

The risk assessment is regularly reviewed and revised. The 04-ISMS Risk Assessment and Risk Treatment Process requires review at least annually. The results of the risk assessment are a mandatory input to the management review conducted by the ISMS Governance Council under 08-ISMS Procedure for Management Review.

REQ-5-05: “The TSP’s management shall approve the risk assessment and accept the residual risk identified.”

The ISMS Governance Council, as the TSP’s management body, approves the risk assessment and accepts the residual risk identified. Approval is documented through the management review process. Unless explicit objection is raised by the Council regarding the Statement of Applicability or Risk Assessment, the SoA and all risk treatment plans are deemed approved following the Management Review.

## **Trust Service Practice Statement [ETSI EN 319 401, clause 6.1]**

Applicable requirement [ETSI EN 319 421, OVR-6.2-01]: “The requirements specified in ETSI EN 319 401, clause 6.1 shall apply.”

The requirements specified in ETSI EN 319 401, clause 6.1 apply to the Hopae Timestamping Service. This CP/CPS constitutes the trust service practice statement. Hopae fulfils these requirements as follows:

REQ-6.1-01: “The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.”

Hopae specifies the set of policies and practices appropriate for the qualified timestamping service it provides. This CP/CPS, structured per RFC 3647, together with the supporting ISMS policies listed in 00-ISMS Master List of Documents, constitutes the complete set of policies and practices.

REQ-6.1-02: “The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.”

The set of policies and practices is approved by the ISMS Governance Council (Section 1.5.3), published in the public repository (Section 2.1), and communicated to employees and external parties as relevant under 06-ISMS Information Security Communication Plan.

REQ-6.1-03X: “The TSP shall have a statement of the practices and procedures used to address all the requirements identified for the applicable TSP’s policy.”

NOTE: The present document makes no requirement as to the structure of the trust service practice statement.

This CP/CPS is the statement of the practices and procedures used to address all the requirements identified for the applicable TSP’s policy. Chapters 1 through 10 of this document address each applicable requirement area. Supporting procedural detail is provided in the ISMS policies referenced throughout.

REQ-6.1-04: “The TSP’s trust service practice statement shall identify the obligations of all external organizations supporting the TSP’s services including the applicable policies and practices.”

This CP/CPS identifies the obligations of all external organizations supporting the TSP’s services, including the applicable policies and practices. INCERT GIE’s obligations are identified in Section 1.1.1 (Delegation Model) and Section 1.3.5 (Other Participants). INCERT maintains its own CP/CPS for the Timestamp Root Certification Authority and is subject to independent conformity assessment. The contractual and oversight framework is governed by Hopae’s Third-Party Management Policy.

REQ-6.1-05X: See Section 1.5.4, Post-Approval Publication.

REQ-6.1-06: See Section 1.5.4.

REQ-6.1-07: See Section 1.5.4.

REQ-6.1-08: See Section 1.5.4, Review Process.

REQ-6.1-09X: See Section 1.5.4, Notification of Changes.

REQ-6.1-10: See Section 1.5.4, Post-Approval Publication.

## 1.6 Definitions and Acronyms

| Term                                       | Definition                                                                                                                                                     |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certification Authority (CA)               | An entity that issues digital certificates                                                                                                                     |
| Certificate Policy (CP)                    | A 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 (CPS)     | A statement of the practices which a Certification Authority employs in issuing, managing, revoking, and renewing or re-keying certificates                    |
| Certificate Revocation List (CRL)          | A list of revoked certificates published by a Certification Authority                                                                                          |
| eIDAS                                      | Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market                                 |
| ETSI                                       | European Telecommunications Standards Institute                                                                                                                |
| Hardware Security Module (HSM)             | A physical computing device that safeguards and manages digital keys and provides crypto-processing                                                            |
| Object Identifier (OID)                    | A globally unique identifier for objects in a hierarchical namespace                                                                                           |
| Public Key Infrastructure (PKI)            | A framework for creating, managing, distributing, using, storing, and revoking digital certificates                                                            |
| Qualified Trust Service Provider (QTSP)    | A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body                         |
| Timestamping Authority (TSA)               | An entity that issues timestamp tokens                                                                                                                         |
| Trust Service Provider (TSP)               | A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider                         |
| Timestamp Token (TST)                      | A data structure that binds a representation of data to a particular time, thus establishing evidence that the data existed at that time                       |
| Qualified Signature Creation Device (QSCD) | An electronic signature creation device that meets the requirements laid down in Annex II of the eIDAS Regulation                                              |

Full glossary and acronym list is provided in Chapter 10.

## 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

### 2.1 Repository Access

Hopae publishes the following information in its publicly accessible repository:

- This CP/CPS document and its updates
- Service terms and conditions
- Contact information for incident reporting
- Termination Plan (summary)
- Service status information

The URL for Hopae's repository is: <https://trust.hopae.com/>

Additionally, INCERT publishes in its public repository:

- The Timestamp Root Certification Authority certificate
- Certificate Revocation Lists (CRLs) issued by the Timestamp Root Certification Authority
- INCERT's Timestamp Root Certification Authority CP/CPS
- Audit reports and other applicable compliance documentation (when approved for publication)

The URL for INCERT's repository is: <https://repository.incert.lu/>

## 2.2 Publication of Certification Information

The Timestamp Root Certification Authority operated by INCERT ensures timely publication of the following information:

- The self-signed Timestamp Root Certification Authority certificate
- CRLs issued by the Timestamp Root Certification Authority, with a maximum validity of 6 months and regular updates to ensure revocation information remains available
- Updates or modifications to the CP/CPS document
- Contact details for the Trust Service Provider 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.

Hopae publishes:

- This CP/CPS upon initial approval and upon each substantive revision
- Service status for real-time availability monitoring
- Incident notifications as required

### Trust Service Documentation Framework:

- This CP/CPS
- Trust Service Termination Plan
- OID Management Policy and Procedure
- INCERT Outsourcing Agreement
- Subscriber Terms and Conditions (published at [trust.hopae.com](https://trust.hopae.com))
- Supporting ISMS policies per 00-ISMS Master List of Documents

## 2.3 Time or Frequency of Publication

- **Timestamp Root Certification Authority Certificate:** Published immediately upon creation and remains available as long as the Certification Authority 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 supervisory 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, including:

- Access control lists restricting modification rights
- Audit logging of all changes
- Integrity verification mechanisms

## 3. IDENTIFICATION AND AUTHENTICATION

This chapter addresses naming and identity validation requirements. Since the Hopae Timestamping Service does not issue certificates to end users, many traditional certificate-related identification requirements are not applicable. However, relevant requirements for subscriber onboarding and TSA certificate naming are addressed.

### 3.1 Naming

#### 3.1.1 Types of Names

The TSA certificate issued by INCERT uses X.500 Distinguished Names (DNs) as defined in RFC 5280. The names are structured to ensure unambiguous identification of the TSA.

The DN of the TSA certificate includes the following attributes:

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

The TSA DN clearly identifies Hopae as the service provider for the timestamping service.

Since timestamping services do 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 timestamp token issued

#### 3.1.2 Need for Names to be Meaningful

The DN attributes are selected to be meaningful and to clearly identify Hopae as the operator of the Timestamping Service in accordance with applicable policy and legal requirements.

### *3.1.3 Anonymity or Pseudonymity of Subscribers*

Not Applicable. The TSA certificate is issued to Hopae as an organization, not to individuals. The Timestamp Root Certification Authority does not issue end-entity certificates to natural persons or pseudonymous identities. Subscriber anonymity at the token request level is not applicable as subscribers must be contractually identified.

### *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*

INCERT's Timestamp Root Certification Authority ensures that the DN of each certificate it issues is unique within its namespace.

### *3.1.6 Recognition, Authentication, and Role of Trademarks*

Hopae and INCERT ensure 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*

TSA private keys are generated and held in HSMs operated by INCERT. The Timestamp Root Certification Authority proves possession of the private key during self-signed certificate generation and through the secure operation of cryptographic modules (HSMs).

For the TSA certificate, INCERT generates the key pair within a Qualified Signature Creation Device (QSCD), and the Certificate Signing Request (CSR) is submitted to the Timestamp Root Certification Authority. Possession is proven through the secure key ceremony process and ongoing HSM controls.

Hopae does not directly possess TSA private keys.

### *3.2.2 Authentication of Organization Identity*

Prior to TSA certificate issuance, INCERT validates Hopae's organizational identity. The organization undergoes:

- Verification of legal identity through official registration documents
- Validation of operational readiness
- Conformance to applicable audit requirements (ETSI EN 319 403)
- Contractual agreement establishing the delegation relationship

### *3.2.3 Authentication of Individual Identity*

Not Applicable. The TSA certificate is issued to Hopae as an organization, not to individuals. The Timestamp Root Certification Authority is not associated with a natural person.

### *3.2.4 Non-Verified Subscriber Information*

Not Applicable. All information in the TSA certificate is verified. The only subscribers to the Timestamp Root Certification Authority are TSA authorities which are identified and authenticated using internal procedures.

### 3.2.5 Validation of Authority

Hopae provides documented evidence of authorization to act as the Qualified Trust Service Provider, including official registration and mandate to provide trust services.

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

### 3.2.6 Criteria for Interoperation

The timestamping service may interoperate with other infrastructures (e.g., EU Trusted 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 with Hopae
- Verification of organization identity and affiliation
- Confirmation of technical integration requirements
- Authorization to submit timestamp requests

### 3.2.8 Key Possession and Validation for Timestamping Services

TSA private keys are securely generated and stored in certified HSMs by INCERT. The possession of these keys is verified internally, under dual control, and during compliance audits. INCERT remains the custodian of TSA keys on behalf of Hopae.

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 TSA certificate is planned well in advance and is conducted by INCERT under strict security controls. Hopae must authorize any re-keying request. The process includes:

- Generation of a new key pair in a secure HSM environment
- Issuance of a new TSA certificate by the Timestamp Root Certification Authority
- Coordinated transition to ensure service continuity

The same security requirements apply for re-keying of the Timestamp Root Certification Authority certificate.

Routine re-key requests follow the same authentication procedures as initial requests; authorization is verified through the established dual-control process. Re-key after revocation requires additional authorization from the ISMS Governance Council and follows incident response procedures if the revocation was due to key compromise.

## 3.4 Identification and Authentication for Revocation Requests

Revocation of the TSA certificate is an exceptional event and would be initiated only under critical circumstances such as key compromise or cessation of service. Revocation requests must:

- Originate from authorized Hopae personnel or be triggered by INCERT security procedures
- Be validated through multi-factor administrative controls

- Be documented and reported to the supervisory authority

Requests must be authenticated via multi-factor procedures or digitally signed by at least 2 authorized personnel.

## 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 Certification Authority, including certificate application, issuance, acceptance, use, renewal, modification, re-key, 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 Timestamping Authority (TSA).

This section also covers the operational activities undertaken by the timestamping service to ensure the secure, reliable, and standards-compliant issuance of timestamp tokens (TSTs). These activities are essential to establishing temporal evidence that can be used for long-term data integrity, legal proof, and regulatory compliance.

Certificate lifecycle management is delegated to INCERT, while Hopae retains governance and authorization responsibility.

### 4.1 Certificate Application

#### 4.1.1 Who Can Submit a Certificate Application

Only authorized personnel within Hopae, specifically designated to manage the lifecycle of the Timestamping Authority, are permitted to submit certificate requests to INCERT for the Timestamp Root Certification Authority. No external entities or third parties are allowed to request certificates from the Timestamp Root Certification Authority.

The request is submitted through the established contractual relationship between Hopae and INCERT.

#### 4.1.2 Enrollment Process and Responsibilities

The TSA certificate application process:

- Hopae authorizes the certificate request through the ISMS Governance Council
- INCERT generates the TSA key pair within a Qualified Signature Creation Device (QSCD)
- A Certificate Signing Request (CSR) is generated by INCERT, complying 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
- INCERT validates the request and issues the TSA certificate
- The Timestamp Root Certification Authority logs all relevant events and maintains an auditable trail for the request process

The TSA key and CSR are generated as part of a key ceremony with witnesses to guarantee the certificate is generated and used in a controlled way.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

INCERT relies on the contractual relationship with Hopae and 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 QSCD
- Ensuring that the requesting entity is an approved component within the organizational PKI hierarchy
- Confirming authorization from Hopae

### 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 Certification Authority personnel
- Audit trail creation

Applications that do not comply with predefined technical and organizational requirements are rejected, and the rejection is recorded in the Certification Authority logs.

### 4.2.3 Time to Process Certificate Applications

Certificate applications shall be processed in a timely manner, typically within five business days following Hopae's authorization and INCERT's technical validation. The issuance timeframe may be extended based on internal security checks or technical validation requirements.

## 4.3 Certificate Issuance

### 4.3.1 Certification Authority Actions During Certificate Issuance

INCERT performs the following actions during TSA certificate issuance:

- Validates the CSR against internal policies
- Ensures the certificate content is compliant with ETSI requirements (ETSI EN 319 411-1, 319 421)
- Signs the certificate using the Timestamp Root Certification Authority'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 Certification Authority repository

### 4.3.2 Notification to Subscriber by the Certification Authority of Issuance of Certificate

INCERT notifies Hopae upon successful TSA certificate issuance through secure communication channels. The issued certificate is imported into the TSA's QSCD in a controlled manner and under the supervision of authorized personnel.

Hopae acknowledges receipt and confirms the certificate is operational.

## 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 INCERT's QSCD by authorized personnel
- Hopae verifies the certificate content (subject DN, key usages, policy OIDs) is correct
- The certificate is actively used to sign timestamp tokens 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, Hopae acknowledges that:

- The certificate content 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 Certification Authority*

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

- The TSA certificate (in DER format)
- The Timestamp Root Certification Authority certificate
- Any applicable CRLs issued by the Certification Authority

#### *4.4.3 Notification of Certificate Issuance by the Certification Authority to Other Entities*

As the Timestamp Root Certification Authority and TSA are components of the same TSP infrastructure under the delegation model, no external notification is typically required. However, relevant information (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 Certification Authority is restricted to the generation of qualified electronic timestamps, in accordance with:

- ETSI EN 319 421
- This CP/CPS and INCERT's CP/CPS
- The constraints encoded in the certificate itself (Key Usage = digitalSignature, Extended Key Usage = timeStamping)

The private key must be stored and used exclusively within a QSCD operated by INCERT, and any operation using this key must be authorized and logged.

For the TSA, the keys can only be used for digital signature, with the Extended Key Usage defined as timeStamping (OID 1.3.6.1.5.5.7.3.8).

#### *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 Hopae and INCERT.

## 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 Hopae personnel may initiate the renewal request, subject to internal policy and dual-control approval. INCERT must authorize execution of the renewal.

### 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

Hopae is notified upon successful renewal through secure communication channels. Installation and activation follow internal documented procedures.

### 4.6.5 Conduct Acceptance of a Renewed Certificate

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

### 4.6.6 Publication of the Renewal Certificate by the Certification Authority

Renewed certificates are published in INCERT's repository alongside the original.

### 4.6.7 Notification of Certificate Issuance by the Certification Authority to Other Entities

Same as Section 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 Timestamp Root Certification Authority certificate

### 4.7.2 Who May Request Certification of a New Public Key

Only authorized Hopae personnel may initiate a certificate re-key request. This request must be approved by the ISMS Governance Council and supported by documented justification.

#### *4.7.3 Processing Certificate Re-Keying Requests*

The re-keying process involves:

- INCERT generates a new key pair using the same QSCD as the original or a newly certified QSCD
- Submission of a new Certificate Signing Request (CSR) to the Timestamp Root Certification Authority
- Review of the request by Timestamp Root Certification Authority 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 personnel. 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 Certification Authority*

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

#### *4.7.7 Notification of Certificate Issuance by the Certification Authority 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 authorized Hopae 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 INCERT 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*

Hopae is notified via secure communication channels 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 Certification Authority*

Published as a new certificate in INCERT's public repository. Old versions will be archived indefinitely.

#### *4.8.7 Notification of Certificate Issuance by the Certification Authority 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 the 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
- Hopae or the timestamping service ceases operations or is restructured
- Regulatory or supervisory directives require such action

#### *4.9.2 Who Can Request Revocation*

Revocation can be initiated by:

- Authorized Hopae personnel
- INCERT (in case of detected compromise or operational issues)
- Regulatory or 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 personnel
- Documented in the incident response and Certification Authority 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 Certification Authority Must Process the Revocation Request*

INCERT 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 INCERT

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 Certification Authority 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*

Hopae publishes information regarding TSA key compromise, revocation, and renewal for subscribers and relying parties on its public repository and status page.

#### *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
- Subscribers and relying parties are notified through published channels

#### *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.

### **4.10 Certificate Status Services**

The Timestamp Root Certification Authority 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 Certification Authority
- **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 24/7 with high availability infrastructure, including redundant web servers and monitored publication jobs.

## 4.11 Timestamp Request Handling

The Hopae Timestamping Service 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 timestamp 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.

## 4.12 Timestamp Token Generation and Response

Upon receiving a valid and authenticated request, the timestamping service 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 ( $\pm 1$  second).

### 4.12.2 Token Construction

A timestamp 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) operated by INCERT. 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.

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

### 4.13 Token Validity and Certificate Revocation

Timestamp 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, Hopae and INCERT will:

- Immediately revoke the certificate and publish its status through CRLs
- Inform subscribers about the TSA being compromised and revoked, through 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.

### 4.14 Service Continuity and Availability

The Hopae Timestamping Service is architected for high availability and fault tolerance, incorporating:

- Redundant timestamping units operated by INCERT
- Automated failover mechanisms
- 24/7 monitoring

Hopae commits to maintaining timestamping service availability as per its Service Level Objectives (SLOs) and contractual agreements with subscribers. Defined SLO targets: 99.9% availability.

Planned downtimes are announced in advance. Unplanned service interruptions are recorded in the audit trail and incident reports, and may trigger incident response procedures.

### 4.15 Notification of Changes in Trust Service Provision

Recipients and channels:

- Subscribers: email to registered contact
- Relying parties: publication at [trust.hopae.com](https://trust.hopae.com)
- ILNAS: official correspondence

- INCERT GIE: written notice per Outsourcing Agreement
- CAB: email to designated contact

Changes requiring notification:

- Cryptographic algorithm/key/certificate profile changes
- Service availability or SLA changes
- Outsourcing arrangement changes
- Planned maintenance exceeding 4 hours
- Intent to cease the qualified trust service

Timeframes:

- Material changes: 30 calendar days advance notice
- Emergency/security: without undue delay, max 24 hours
- Planned maintenance: 30 calendar days
- Termination: per Termination Plan §5

Responsible: Head of Trust & Security Officer

Records: Notification log maintained as ISMS evidence.

#### *4.15.1 Notification to Supervisory Authority (Article 21(1))*

Per Article 21(1) of the Implementing Regulation, Hopae shall notify ILNAS of any changes to elements impacting the Trusted List entry or trust service provision. Each notification shall include:

1. Description of the change
2. Planned date and time
3. Reasons and evidence where applicable
4. Updated documents where applicable

Notifiable categories (Article 21(1)(a)-(j)): CP/CPS changes, technical architecture, hosting, cryptographic changes, registration procedures, governance, termination plan, insurance/financial, Trusted List-impacting changes, third-party/subcontractor changes.

Timing: Before the change takes effect (planned), or without undue delay (unplanned).

In accordance with Directive (EU) 2022/2555 (NIS2) Article 23, significant incidents affecting the timestamping service are additionally reported to the competent authority within the following timelines: early warning within 24 hours, incident notification within 72 hours, and a final report within one month of the incident.

Responsible: Head of Trust & Security Officer

Delivery: Official correspondence (email + registered mail if required by ILNAS)

Template: Maintained as ISMS controlled document.

## **5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS**

This section outlines the physical, procedural, and personnel security measures implemented to protect the timestamping service 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.

**Critical Note:** As described in Section 1.1.1 (Delegation Model), Hopae does not operate physical data centers or HSM infrastructure. Physical and technical controls for the TSA cryptographic infrastructure are implemented by INCERT per their CP/CPS and audit requirements. Hopae maintains governance, oversight, and administrative controls.

## 5.1 Physical Security

Physical security for the TSA infrastructure is implemented by INCERT. The following describes INCERT's controls as documented in their CP/CPS.

### 5.1.1 Site Location and Construction

INCERT hosts the Timestamp Root Certification Authority and TSA in a secure, access-controlled data center facility designed to meet Tier III or higher standards. The data center 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 (Hardware Security Modules — HSMs)
- Multi-layer perimeter security with monitored entry points

The same data center hosts the systems related to the TSA but remains online, while the Timestamp Root Certification Authority is stored offline or semi-offline so that it's isolated and accessible only by trusted personnel under dual control procedures.

### 5.1.2 Physical Access

Access to Timestamp Root Certification Authority and TSA facilities is strictly limited to authorized personnel and is protected through:

- Biometric access control and smart card authentication
- 24/7 surveillance (CCTV), with video retention as per data center 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 at INCERT premises.

### 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

INCERT defines the following trusted roles for TSA operations:

- **Certification Authority Administrator:** Manages Certification Authority 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 (operating system, database)

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

Hopae defines the following governance roles:

- **Head of Trust & Security Officer:** Responsible for QTSP compliance and oversight of the timestamping service
- **Data Protection Officer:** Privacy and data protection oversight, independent advisor to management
- **ISMS Governance Council:** Policy approval, strategic direction, and management review

### Trusted Role Descriptions

#### Security Officer

- Holder: Junmin Kim (Eric Kim) (Head of Trust / ISMS Manager)
- Qualifications: ISO 27001 Lead Implementer/Auditor or equivalent; eIDAS/ETSI knowledge; 3+ years information security
- Duties: Policy governance, QTSP compliance, conformity assessment coordination, incident oversight, INCERT oversight, risk management, OID management
- Segregation: Shall not perform System Operator or System Administrator functions
- Backup: CEO (limited operational continuity)

#### System Administrator

- Holder: INCERT GIE personnel
- Qualifications: HSM/PKI administration experience; 3+ years systems administration in trust services
- Duties: HSM management, server administration, network configuration, backup/recovery, patching
- Segregation: Shall not perform Security Officer or System Auditor functions
- Backup: INCERT internal rotation

#### System Operator

- Holder: INCERT GIE (coordinated by Hopae Operations)

- Qualifications: TSA/PKI operations experience; ETSI EN 319 421 training
- Duties: TSA operations, timestamp signing, CRL generation, operational monitoring
- Segregation: Shall not perform System Administrator functions
- Backup: INCERT internal rotation

### System Auditor

- Holder: Patrick Bosch (External System Auditor)
- Qualifications: ETSI EN 319 403 qualified auditor; independence from all operational roles
- Duties: Conformity assessment, internal audit support
- Segregation: Independent from all other roles

Role descriptions maintained per REQ-7.2-09X. INCERT personnel meet equivalent standards per Outsourcing Agreement.

Note: Technical operations are delegated to INCERT per ETSI EN 319 401 REQ-7.1.1-07. Staffing levels reviewed as service portfolio expands.

#### *5.2.2 Number of Persons Required per Task*

At INCERT:

- 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

At Hopae:

- Policy changes require ISMS Governance Council approval
- Incident escalation follows defined procedures with multiple authorization levels

#### *5.2.3 Identification and Authentication for Each Role*

- Personnel are authenticated using multi-factor authentication (e.g., smart card + PIN)
- Access to Certification Authority 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:

- At INCERT, the roles of Security Officer and Certification Authority Administrator are strictly separated
- No single individual may hold roles across both operations and audit/compliance
- At Hopae, the Head of Trust and Data Protection Officer maintain independent oversight functions

All trusted role appointments are formally executed in writing by the CEO prior to commencement of qualified trust service operations, per the Formal Appointment Process in 03-ISMS Roles, Responsibilities, and Authorities.

## 5.3 Personnel Controls

### *5.3.1 Qualifications, Experience, and Clearance Requirements*

Personnel assigned to trusted roles at both INCERT and Hopae 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

Personnel in trusted roles fulfil the requirement of 'expert knowledge, experience and qualifications' (REQ-7.2-04X; OVR-7.3-02) through formal training and credentials, actual experience, or a combination of the two. Evidence documented in personnel files; reviewed annually.

### *5.3.2 Background Check Procedures*

Background checks are conducted prior to onboarding into trusted roles, including:

- Identity verification
- Employment and education history verification
- Criminal background screening

Personnel shall not have access to trusted functions until all required checks are completed (REQ-7.2-17).

### *5.3.3 Training Requirements*

All personnel receive:

- Information security awareness (annual, via Vanta)
- GDPR and data protection (annual, via Vanta)
- Secure development practices (annual, Engineering/Operations, via Vanta)
- Role-specific technical training (as needed)

Personnel in trusted roles additionally complete:

- Trust service-specific training: eIDAS regulatory framework, ETSI EN 319 401/421 requirements, CP/CPS content, incident response, key ceremony procedures. Delivered by ISMS Manager, annually and upon material policy changes.

INCERT personnel training requirements per Outsourcing Agreement.

### *5.3.4 Retraining Frequency and Requirements*

Retraining at least annually, including updates on new threats and current security practices (OVR-7.3-03). Training records maintained per REQ-7.2-12X. Attendance mandatory and documented.

### *5.3.5 Job Rotation Frequency and Sequence*

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

### *5.3.6 Sanctions for Unauthorized Actions*

Level 1 (Minor — unintentional, no security impact): Verbal warning + mandatory refresher training.

Level 2 (Moderate — repeated minor or potential security impact): Written warning + enhanced monitoring + retraining within 10 business days.

Level 3 (Serious — actual security impact, willful misconduct, deliberate circumvention): Immediate access revocation + investigation + written warning, suspension, or termination + potential legal proceedings.

For INCERT personnel: equivalent provisions per Outsourcing Agreement. Hopae may request removal for Level 3.

#### *5.3.7 Independent Contractor Requirements*

Contractors in trusted roles must:

- Sign non-disclosure agreements (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 Certification Authority and the TSA to protect its cryptographic keys, systems, and data. These controls ensure the confidentiality, integrity, and availability of the timestamping service in line with ETSI EN 319 411-1/2 and ETSI EN 319 421.

**Critical Note:** As described in Section 1.1.1 (Delegation Model), Hopae does not operate HSMs or generate TSA keys directly. All cryptographic operations are performed by INCERT.

### **6.1 Key Pair Generation and Installation**

#### *6.1.1 Key Pair Generation*

Timestamp Root Certification Authority and TSA key pairs are generated within a FIPS 140-2 Level 3 or Common Criteria EAL4+ certified Hardware Security Module (HSM).

Generation of the Timestamp Root Certification Authority key pair is performed in a formal key ceremony, witnessed and recorded, with dual control and multi-person integrity (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*

Not Applicable. The Timestamp Root Certification Authority does not deliver private keys to any external entity. TSA private keys are never delivered outside INCERT's HSMs. Hopae does not receive or possess TSA private keys.

The TSA's certificate will be issued by the Timestamp Root Certification Authority, but the TSA key pair will be generated independently by INCERT within the QSCD, and the Certificate Signing Request (CSR) will be submitted to the Timestamp Root Certification Authority.

#### *6.1.3 Public Key Delivery to Certificate Issuer*

For the Timestamp Root Certification Authority, as a self-signed Certification Authority, this does not apply.

For the TSA, the public key is handled for certificate issuance as part of INCERT's formal key ceremony process.

#### *6.1.4 Certification Authority Public Key Delivery to Relying Parties*

The Timestamp Root Certification Authority certificate is made publicly available through:

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

#### *6.1.5 Key Sizes and Algorithms*

Key sizes and algorithms (per INCERT certificate profiles):

Timestamp Root Certification Authority:

- Key: ECC P-384 (secp384r1)
- Signature Algorithm: ECDSA with SHA-384

TSA Certificate (End Entity):

- Key: ECC P-256 (secp256r1)
- Signature Algorithm: ECDSA with SHA-256

These parameters are defined by INCERT's certificate profile and comply with SOG-IS 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 Certification Authority 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 digital signature, with the Extended Key Usage defined as timeStamping (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 Timestamp Root Certification Authority 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 at INCERT.

### *6.2.3 Private Key Escrow*

Not Applicable. Timestamp Root Certification Authority and TSA private keys are never escrowed under any circumstances.

### *6.2.4 Private Key Backup*

Keys are backed up by INCERT in encrypted form and stored in a safe located in an access-controlled secure location, such as INCERT premises.

Backup media is handled only during a key ceremony and stored in an access-controlled secure location.

### *6.2.5 Private Key Archival*

Not Applicable. Archival of private keys is not practiced for the Timestamp Root Certification Authority or TSA.

Expired 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 secured as defined in Section 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 Certification Authority:

- 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 handle operations, but their usage is strictly controlled and logged for traceability.

### *6.2.9 Method of Deactivating Private Key*

- Timestamp Root Certification Authority keys are automatically deactivated after operations or upon session timeout
- The HSM (for both Timestamp Root Certification Authority 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 upon 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 Certification Authority's public key and associated certificate are archived for a minimum of 20 years after the expiration or revocation of the Timestamp Root Certification Authority 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 Certification Authority's operational lifetime.

### 6.3.2 Certificate Operational Periods and Key Usage Periods

- Timestamp Root Certification Authority certificate validity: 20 years from key ceremony date
- Timestamp Root Certification Authority key usage: limited to 19 years with 1 year overlap for transition
- TSA certificates have a validity period of 1 year from key ceremony date, as defined in INCERT's certificate profile

## 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 at INCERT.

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

INCERT implements:

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

Hopae implements:

- Security controls per ISO 27001 Information Security Management System
- Cloud infrastructure security (AWS) per documented policies
- Access control and monitoring as defined in Hopae's ISMS policies

### Configuration Compliance Checks (REQ-6.3-08X / REQ-6.3-09X)

The configuration of TSP systems is regularly checked for changes that violate the TSP's security policies:

- Hopae-managed systems: at least annually (network access rules); at least quarterly (vulnerability scans on public-facing systems). Continuous monitoring via Amazon Inspector, GuardDuty, and Vanta.
- INCERT-managed TSA infrastructure: at least annually per the Outsourcing Agreement. Configuration compliance reports provided to Hopae following each check.

Maximum check interval: annually (documented per REQ-6.3-09X).

The asset inventory is reviewed at planned intervals, at least annually, per REQ-6.3-06X.

The information security policy is approved by the ISMS Governance Council. Approval and review procedures follow Section 1.5.4 of this CP/CPS and 05-ISMS Procedure for the Control of Documented Information.

Maintenance procedures for INCERT-managed TSA assets (HSMs, servers, time sources) are governed by INCERT's information security policy and documented in the Outsourcing Agreement.

## 6.6 Life Cycle Technical Controls

### 6.6.1 System Development Controls

Certification Authority software and scripts are developed in-house or obtained from verified vendors by INCERT.

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 Certification Authority are tracked through asset management
- Decommissioning of systems follows secure erasure and physical destruction protocols

## 6.7 Network Security Controls

Certification Authority systems operate on segmented, firewalled networks with:

- Strict ingress/egress rules
- Only pre-approved IP ranges and ports allowed
- Intrusion Detection and Prevention Systems (IDPS) monitoring network traffic

## 6.8 Time-Stamping

Timestamp tokens are not applicable for the Timestamp Root Certification Authority, as it does not issue timestamp tokens directly. The date/time used at the Timestamp Root Certification Authority servers is still synchronized with the internal trusted NTP servers.

Timestamping responsibilities are handled by the TSA, which receives its certificate from the Timestamp Root Certification Authority.

### 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  $\pm 1$  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 timestamp 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 ten (10) years, in accordance with eIDAS requirements for qualified trust services; other records are retained per the GRC Retention Register
- 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 Certification Authority, as well as the structure and content of Certificate Revocation Lists (CRLs). Since the Timestamp Root Certification Authority does not provide an Online Certificate Status Protocol (OCSP) service, OCSP profiles are noted as not applicable.

### 7.1 Certificate Profile

#### 7.1.1 Version Number

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

#### 7.1.2 Certificate Extensions

The standard extensions included in the Timestamp Root Certification Authority certificate are documented in INCERT's naming and profile documentation per ETSI requirements.

#### 7.1.3 Algorithm and Key Length

ECC P-384 with ECDSA and SHA-384, compliant with SOG-IS and eIDAS requirements.

#### 7.1.4 Name Forms

The subject Distinguished Name is documented in INCERT's naming and profile documentation, clearly identifying Hopae as the TSA operator.

#### 7.1.5 Certificate Validity Period

- The Timestamp Root Certification Authority certificate typically has a validity period of 20 years from key ceremony date, as defined in INCERT's certificate profile, 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 Timestamp Root Certification Authority lifetime

#### 7.1.6 Certificate Policy Object Identifier (OID)

The certificate will include the CP OID uniquely identifying this CP/CPS document.

The certificate includes the time-stamp policy OID 1.3.171.7.1.1.1 identifying this CP/CPS, as specified in Section 1.2.

#### 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

The TSA certificate:

- Is issued by the Timestamp Root Certification Authority operated by INCERT
- Contains the Key Usage extension with digitalSignature set
- Includes the Extended Key Usage extension with timeStamping (OID 1.3.6.1.5.5.7.3.8)
- Is bound to this CP through the PolicyIdentifier extension
- Is valid for 1 year from key ceremony date, as defined in INCERT's certificate profile, and subject to controlled renewal
- Is published in the TSA repository and included in signed responses for validation purposes
- Is not used for signing documents, authentication, or TLS but only to issue TSTs

The certificate chain includes:

- TSA Certificate (leaf, qualified for timestamping use)
- Timestamp Root Certification Authority (self-signed)

This hierarchy ensures direct and verifiable trust in timestamp tokens through an audited and published root.

The complete certificate profile is documented by INCERT.

## 7.3 Timestamp Token Structure

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

- A message imprint (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  $\pm 1$  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 Certification Authority are documented in INCERT's naming and profile documentation per ETSI requirements.

### 7.4.3 CRL Issuance Frequency

- The Timestamp Root Certification Authority 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 INCERT'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 Certification Authority 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 timestamping service operates in accordance with applicable standards, regulatory requirements, and the practices set forth in this CP/CPS.

### 8.1 Frequency or Circumstances of Assessment

Hopae is subject to regular compliance audits as the QTSP 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 319 421, and EN 319 411-1
- The practices stated in this CP/CPS, which constitutes the Trust Service Practice Statement

Audit schedule:

- A full conformity assessment is performed prior to initial inclusion of the Timestamp Root Certification Authority certificate in the EU Trusted List
- Following a positive initial conformity assessment, the supervisory authority validates the audit report and facilitates the inclusion of the Timestamp Root Certification Authority 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

INCERT undergoes separate audits for their infrastructure and operations per their CP/CPS. Hopae obtains and reviews INCERT audit reports as part of third-party oversight.

## 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
- Is 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 Hopae
- The CAB has no financial or operational ties that could compromise the impartiality or objectivity of the assessment
- Hopae 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 timestamping service
- Physical and logical security controls
- Certificate lifecycle management (delegated to INCERT)
- Timestamping service operations
- Conformance of certificate profiles to applicable technical standards
- CRL generation, distribution, and retention
- Personnel security and role-based access controls
- Documentation, including CP/CPS and TSPS compliance
- Incident handling and business continuity measures
- Internal audit procedures and quality controls
- Third-party management (oversight of INCERT)

## 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 timestamping service may lead to:

- Temporary suspension of service
- Withdrawal of the Timestamp Root Certification Authority certificate from the EU Trusted List by the supervisory body
- Notification to affected subscribers and relying parties

## 8.6 Communication of Results

- Upon successful audit, the conformity assessment report is submitted to the national supervisory body (ILNAS) for validation
- If validated, the supervisory body facilitates the inclusion of the Timestamp Root Certification Authority certificate in the EU Trusted 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 Hopae Timestamping Service, including liability, fees, intellectual property rights, privacy, and dispute resolution mechanisms.

### 9.1 Fees

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

Fees may be charged to subscribers for:

- Timestamping service access
- Volume-based pricing as defined in service agreements

Fee structures for timestamping services are published separately and detailed in subscriber agreements. Commercial terms are available upon request to subscribers and are subject to periodic review.

ETSI EN 319 421 explicitly states that policy requirements are not meant to imply restrictions on charging for TSA services. Fee disclosure in the CP/CPS is not required by eIDAS or applicable ETSI standards.

### 9.2 Financial Responsibility

Hopae S.A. maintains appropriate financial resources and professional liability insurance coverage as required under Article 24(2)(c) of Regulation (EU) No 910/2014 (eIDAS) and applicable Luxembourg national law for Qualified Trust Service Providers.

#### Insurance Coverage

Hopae holds a Professional Liability insurance policy issued by CNA, structured as a claims-made policy covering claims first made against the insured during the policy period.

This coverage addresses:

- Potential liabilities arising from errors, omissions, or failures in the provision of qualified trust services
- Claims related to timestamping service operations
- Business continuity and disaster recovery obligations

### **Policy Administration**

The insurance policy is maintained in the name of Hopae S.A. at its registered address: 20 Rue des Peupliers, L-2328 Luxembourg, Grand Duchy of Luxembourg.

Policy declarations and warranty statements are executed by an authorized director of the company.

### **Coverage Adequacy**

Hopae performs regular risk assessments to ensure the adequacy of insurance coverage relative to:

- The nature and scope of trust services provided
- Potential liability exposure from service failures
- Regulatory requirements applicable to QTSPs in Luxembourg

Evidence of insurance coverage is maintained and made available to the supervisory authority (ILNAS) and conformity assessment bodies upon request.

Note: Specific coverage limits, policy number, and policy period are documented in the insurance certificate/policy schedule, maintained separately from this CP/CPS and available for audit purposes.

## **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:

- Applicable Luxembourg and EU legislation
- Hopae'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**

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

Personal data collected in the course of trust service provision 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 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 Hopae, unless otherwise stated.

Use of TSA 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

### 9.6.1 Subscriber Obligations (Terms and Conditions)

Subscribers shall:

1. Verify that each time-stamp has been correctly signed and that the private key used to sign was not compromised until the time of verification
2. Take into account any limitations on usage indicated by the time-stamp policy (OID 1.3.171.7.1.1.1)
3. Take into account any other precautions prescribed in this CP/CPS or the Subscriber Agreement
4. Use the service only in accordance with Section 1.4
5. Safeguard API credentials and report suspected compromise without undue delay
6. Comply with applicable laws and regulations

### 9.6.2 Relying Party Obligations

Relying parties shall:

1. Verify the TSA certificate chain to the Timestamp Root CA
2. Check the CRL for revocation status
3. Verify the digital signature on the timestamp token
4. Assess the applicability of the timestamp policy (OID 1.3.171.7.1.1.1)
5. Accept that the timestamp token does not guarantee data accuracy, but only that the data existed at the indicated time

### 9.6.3 Fee Structure

Fee structures are determined by the Subscriber Agreement. These policy requirements do not imply restrictions on charging for TSA services (ETSI EN 319 421).

Terms and Conditions are published at <https://trust.hopae.com/>.

## 9.7 Disclaimers of Warranties

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

Hopae does not warrant that use of the service will be uninterrupted or error-free, or that relying parties will not experience damage or loss.

## 9.8 Limitations of Liability

### 9.8.1 Statutory Framework

Hopae's liability as a Qualified Trust Service Provider is governed by Article 13 of Regulation (EU) No 910/2014 (eIDAS). For qualified trust services, intent or negligence is presumed unless Hopae demonstrates it acted without fault.

### 9.8.2 Liability Cap

Subject to mandatory statutory provisions and to the extent permitted by Luxembourg law, Hopae's aggregate liability for claims arising from the qualified timestamping service shall not exceed EUR 10,000 per calendar year per subscriber.

This cap does not apply to:

- Gross negligence or willful misconduct
- Fraud or intentional damage
- Personal injury or death
- Regulatory fines or penalties (including GDPR)

### 9.8.3 Exclusions

Hopae shall not be liable for:

- Indirect, incidental, or consequential damages
- Loss of profits, revenue, or business opportunities
- Damages arising from relying party failure to verify certificate status via published CRLs
- Force majeure events
- Subscriber misuse or misrepresentation

### 9.8.4 Delegated Operations

Hopae retains full liability to subscribers and relying parties for operations delegated to INCERT GIE. Internal allocation of liability between Hopae and INCERT does not affect third-party rights.

## 9.9 Indemnities

Subscribers and relying parties shall indemnify and hold harmless Hopae for:

- Any misuse of timestamp tokens
- Non-compliance with the terms of this CP/CPS
- Breach of contractual or regulatory obligations

## 9.10 Term and Termination

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

Hopae may terminate its services under conditions such as:

- Voluntary shutdown
- Revocation of QTSP status
- Regulatory order or legal judgment

In such cases, appropriate steps will be taken to:

- Notify affected parties per the Termination Plan
- Coordinate TSA certificate revocation with INCERT
- Maintain repository access for a defined archival period
- Transfer records to the supervisory authority or successor if required

### Termination Plan Review

The Trust Service Termination Plan is reviewed at least annually in the ISMS management review cycle, or following significant changes. Reviews are documented with date, reviewer, and findings.

The termination plan is included in the internal audit cycle per 07-ISMS Procedure for Internal Audits. Scheduling responsibility: ISMS Manager.

### Document Handover

The list of documents to be transferred to a successor TSP is specified in the Termination Plan and in Schedule D of the INCERT Outsourcing Agreement.

## 9.11 Individual Notices and Communications with Participants

Official communications are conducted through:

- Email addresses listed in this CP/CPS
- Hopae's official website and repository

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
- Findings from audits or incidents

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

A change is considered significant where it may impact trust, security objectives, certificate profiles, cryptographic algorithms, delegation arrangements, or compliance with applicable ETSI standards or eIDAS requirements.

## 9.13 Dispute Resolution Provisions

### 9.13.1 Governing Procedure

Disputes shall be resolved through the following tiered process:

1. **Internal Resolution (30 days):** Written complaint submitted to [trust@hopae.com](mailto:trust@hopae.com); response within 30 calendar days
2. **Escalation (15 days):** Unresolved complaints escalated to the ISMS Governance Council
3. **Mediation (optional):** Parties may elect voluntary mediation through the Centre of Civil and Commercial Mediation of Luxembourg (CMCC)
4. **Arbitration (binding):** Disputes not resolved through the above steps shall be finally settled under the Rules of the Luxembourg Arbitration Center (LAC)

### 9.13.2 Arbitration Terms

- Seat of arbitration: Luxembourg
- Language: English or French
- Number of arbitrators: One (1) for disputes under EUR 250,000; three (3) for larger disputes
- Simplified Proceedings apply for disputes under EUR 1,000,000

### 9.13.3 Jurisdiction

Notwithstanding the above, either party may seek injunctive relief from the courts of Luxembourg for urgent matters involving intellectual property or confidentiality breaches.

## 9.14 Governing Law

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

## 9.15 Compliance with Applicable Law

Hopae ensures full compliance with:

- eIDAS Regulation
- General Data Protection Regulation (GDPR)
- Luxembourg national regulations for qualified trust service providers

## 9.16 Miscellaneous 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

## 9.17 Other Provisions

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

## 9.18 ISO/IEC 27701 Privacy Information Management System (PIMS) Addendum

This addendum applies to organizations implementing ISO/IEC 27701:2019 in conjunction with ISO/IEC 27001:2022.

Hopae S.A. acts as Data Processor (or Sub-Processor) for personal data processed through its services and is not the Data Controller of such data; the qualified timestamping service processes only cryptographic hashes, which contain no personal data. A Data Controller role arises only for ancillary corporate processing (workforce administration, business contacts, and the security of Hopae's own systems).

Accordingly:

- All references to "ISMS" in this document shall be read as "ISMS/PIMS."
- ISO/IEC 27701 Annex B (Processors) applies to personal data processed through Hopae's services (customer-directed processing).
- ISO/IEC 27701 Annex A (Controllers) applies only to Hopae's ancillary corporate processing (workforce, business contacts).

Data protection is overseen by the Data Protection Officer (DPO), with governance responsibilities coordinated through the ISMS Governance Council.

## 10. GLOSSARY AND REFERENCE DOCUMENTS

### 10.1 Definitions

See Section 1.6 for definitions of key terms.

### 10.2 Acronyms

| Acronym | Definition                                                   |
|---------|--------------------------------------------------------------|
| API     | Application Programming Interface                            |
| CA      | Certification Authority                                      |
| CAB     | Conformity Assessment Body                                   |
| CP      | Certificate Policy                                           |
| BTSP    | Best Practices Time-Stamping Policy                          |
| CPS     | Certification Practice Statement                             |
| CRL     | Certificate Revocation List                                  |
| DR      | Disaster Recovery                                            |
| eIDAS   | Electronic Identification, Authentication and Trust Services |
| ETSI    | European Telecommunications Standards Institute              |
| GDPR    | General Data Protection Regulation                           |
| HSM     | Hardware Security Module                                     |
| ISMS    | Information Security Management System                       |
| LTV     | Long-Term Validation                                         |
| NTP     | Network Time Protocol                                        |
| OCSP    | Online Certificate Status Protocol                           |
| OID     | Object Identifier                                            |
| PEN     | Private Enterprise Number                                    |
| PKI     | Public Key Infrastructure                                    |
| QSCD    | Qualified Signature Creation Device                          |
| QTSP    | Qualified Trust Service Provider                             |
| RPO     | Recovery Point Objective                                     |
| RTO     | Recovery Time Objective                                      |
| TSA     | Timestamping Authority                                       |
| TSP     | Trust Service Provider                                       |
| TST     | Timestamp Token                                              |

| Acronym | Definition                       |
|---------|----------------------------------|
| TSPS    | Trust Service Practice Statement |
| UTC     | Coordinated Universal Time       |

### 10.3 Reference Documents

| Reference         | Title                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RFC 3161          | Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)                                                                                               |
| RFC 3647          | Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework                                                                |
| RFC 5280          | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile                                                               |
| eIDAS             | Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market                                   |
| ETSI EN 319 401   | Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers                                                         |
| ETSI EN 319 411-1 | Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements |
| ETSI EN 319 421   | Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps                                |
| ETSI EN 319 422   | Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles                                                            |
| ETSI EN 319 403   | Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment                                                                    |
| ISO/IEC 27001     | Information Security Management Systems — Requirements                                                                                                           |

### Version History

| Version | Date       | Summary                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Author                   | Approval                        |
|---------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|---------------------------------|
| 1.2     | 03/09/2026 | Format standardised to Hopae document standard; entity names, roles, DPO and numeric parameters aligned to group baseline (P1 consistency batch). Reconciled against approved v1.1 (Vanta): merged §1.5.4 expansion, §1.5.5 ETSI conformance mapping, §4.15 notification procedures, §5.2.1 trusted role descriptions, §6.5 configuration compliance checks, §9.6.1-9.6.3 subscriber/relying-party obligations, §9.10 termination plan review and document handover, §1.1.2 OID management cross-reference, §1.3.3 subscriber scope. QTSP event-log retention aligned to 10 years per eIDAS with other records per the GRC Retention Register (H-8); legal entity name corrected to Hopae S.A. throughout (C-4); PIMS addendum restated as processor-only for service data per group | Junmin Kim<br>(Eric Kim) | Jaehoon Shim<br>(Ace Shim), CEO |

| Version | Date       | Summary                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Author                   | Approval                   |
|---------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------|
|         |            | GDPR baseline (C-2R, owner determination 02/09/2026); System Auditor designated: Patrick Bosch (owner confirmation 03/09/2026); duplicative v1.0 'Change Management Alignment' block removed from §1.5.4 (superseded by REQ-6.1 mappings, owner confirmation 03/09/2026). Merged from unapproved Vanta draft (Apr 2026): NIS2 Directive compliance statement (§1.1.3), NIS2 Article 23 incident-notification timelines (§4.15.1), BTSP OID 0.4.0.2023.1.1 reference (§1.2), ETSI EN 319 422 coverage reference, and re-key authorization provisions (§3.3). |                          |                            |
| 1.1     | 16/02/2026 | Pre-audit conformity response: Added T&C framework, notification procedures, configuration check intervals, OID management cross-reference, trusted role job descriptions, subscriber scope clarification, INCERT contractual alignment, termination plan document list.                                                                                                                                                                                                                                                                                    | Junmin Kim<br>(Eric Kim) | Jaehoon Shim<br>(Ace Shim) |
| 1.0     | 08/01/2026 | Initial version                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Junmin Kim<br>(Eric Kim) | Jaehoon Shim<br>(Ace Shim) |

— End of Document —