incode psc

QTSP Timestamp Policy / Statement

Version	Modified by	Modifications made	Date modified
1.0	LV	Content	02/2025

Tabla de contenido

1. Introduction

In today's digital landscape, organizations that rely on information systems, electronic transactions, or structured data frameworks require trustworthy and verifiable evidence to ensure the authenticity, integrity, and precise timing of their data. Establishing a reliable and legally recognized link between the moment data is generated or a transaction occurs, and its certified timestamp is essential for legal compliance, security, and non-repudiation in digital environments.

This Qualified Timestamp Policy and Statement, in accordance with ETSI EN 319 421, defines the principles, operational framework, and security measures governing the issuance, validation, and management of qualified timestamps. These timestamps serve as irrefutable proof that specific data or transactions existed at a particular date and time, ensuring auditability, regulatory compliance, and long-term data integrity.

By adhering to this policy, Incode ensures that its timestamping services provide a highly reliable, cryptographically secure, and legally admissible mechanism for time validation, supporting organizations in maintaining trust and compliance in digital transactions..

2. Scope

This Qualified Timestamp Policy and Practices Statement (QTPS) sets forth the requirements and operational guidelines for Incode, as a Qualified Trust Service Provider (QTSP), responsible for issuing qualified digital timestamps in accordance with international standards and regulatory frameworks.

It defines the technical and procedural mechanisms that ensure timestamps are:

- Cryptographically secure and resistant to tampering.
- Issued with a precise, verifiable time reference linked to an official time source.
- Compliant with RFC 3161, ETSI EN 319 421, and eIDAS Regulation (EU 910/2014).

The Timestamp Authority (TSA) operates within the Public Key Infrastructure (PKI) model, ensuring that all timestamps are generated, managed, and validated through a secure, controlled, and auditable environment.

3. Definitions of Terms and Abbreviations

3.1 Terms

Term	Definition
Coordinated Universal Time (UTC)	Time scale based on the second as defined in Recommendation ITU-R TF.460-6
Relying Party	Legal or natural person that relies on a timestamp provided by Incode as QTSP.
Subscriber	A legal or natural person to whom a timestamp is issued and who is responsible for fulfilling any subscriber obligations.
Timestamp	A timestamp is a cryptographically secure record that certifies the existence of specific data at a particular point in time.
Timestamp Policy	Set of rules that indicates the applicability of a timestamp with common security requirements
Time-Stamping Authority (TSA)	A Trusted Authority, either a TSP or QTSP, that provides timestamp services using one or more TSUs.
Time-Stamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single timestamp signing key active at a time
UTC(K)	Time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns

3.2 Abbreviations

Abbreviation	Definition
BIMP	Bureau International des Poids et Mesures
CA	Certification Authority
HSM	Hardware Security Module
PKI	Public Key Infrastructure
QTSP	Qualified Trust Service Provider
TIS	Time-stamp Issuance Services
TSA	Time-StampingAuthority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time
VPN	Virtual Private network

4. General concepts

4.1 General Policy Requirement Concepts

Incode TSA operates its timestamping services in full compliance with ETSI EN 319 421 and any other applicable regulations, including but not limited to:

- eIDAS Regulation (EU) No 910/2014
- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers)
- National laws and industry best practices applicable to timestamping services

Incode TSA ensures that all timestamps issued are legally recognized and admissible as evidence within applicable jurisdictions.

4.1.1 Trustworthiness of the Timestamping Service

Incode TSA ensures that the timestamping service operates in a secure, reliable, and trustworthy manner, providing timestamps that guarantee:

- The authenticity and integrity of the timestamped data.
- Protection against unauthorized modification or falsification of timestamps.
- Traceability to a secure and recognized time source.

Appropriate security controls shall be implemented to detect, mitigate, and prevent any threats that could compromise the trustworthiness of the service.

4.2 Timestamp services

The Timestamping Authority (TSA) is responsible for providing trusted time-stamping services in accordance with this policy. These services are categorized into two primary components:

4.2.1 Timestamp Generation Service

The Time-Stamp Generation Service is responsible for issuing time-stamp tokens in response to valid requests. Each issued time-stamp token binds a cryptographic hash of the submitted data to an accurate time source, ensuring that the existence of the data at a specific point in time can be cryptographically proven.

Incode service must:

- Ensure that all time-stamps are generated in compliance with RFC 3161 (Internet X.509 PKI Time-Stamp Protocol) and ETSI EN 319 421 requirements.
- Guarantee that the time included in the token is synchronized with Coordinated Universal Time (UTC) using a trusted time source.

- Ensure the integrity, authenticity, and non-repudiation of each time-stamp token issued.

4.2.2 Timestamp Management Service

The Timestamp Management Service oversees the administration, security, and operational integrity of the time-stamping infrastructure. This service includes:

- Time Source Synchronization: Incode TSA ensures that its clock remains accurate and traceable to UTC, with regular synchronization and monitoring to maintain compliance with precision requirements.
- Key Management: Incode TSA is responsible for securely managing its private signing keys, including key generation, storage, and periodic rotation as per security policies.
- Audit Logging and Monitoring: All timestamp requests, issuances, and system events are securely logged and auditable to maintain compliance.
- System Availability and Continuity: Incode TSA implement redundancy and disaster recovery mechanisms to ensure the continuous availability of the time-stamping service.

4.2.3 Responsibility and Oversight

Incode TSA retains full responsibility for the proper operation and compliance of the timestamping services, even in cases where certain operational aspects are delegated to third parties. Any delegation must be performed under contractual agreements that ensure compliance with this policy and relevant regulations.

4.3 Timestamp Authority

The Timestamping Authority is responsible for delivering time-stamping services to subscribers. The TSA holds comprehensive responsibility for the provision and management of these services, ensuring their integrity, accuracy, and compliance with established policies.

Incode TSA manages one or more TSUs, which are systems comprising hardware and software designed to generate and sign time-stamps on behalf of the TSA. Each TSU operates under a unique time-stamp signing key, ensuring the authenticity and traceability of issued time-stamps.

Incode TSA must be clearly identifiable in each time-stamp it issues, providing assurance to relying parties regarding the source and trustworthiness of the time-stamp.

4.4 Subscribers

All individuals or organizations with a legitimate interest in requesting digital timestamps and who have completed the contractual agreement process with Incode for recurring access to the service are recognized as subscribers of the TSA service.

Subscribers of the TSA service acknowledge and accept the responsibilities and obligations of the TSA, as well as the responsibilities and obligations they assume as users of the service and the use of the timestamp tokens they request and are provided with.

4.5 Relying parties

Individuals, organizations, or systems that trust and depend on timestamps issued by QTSP to verify the authenticity, integrity, and existence of data at a specific point in time. These parties do not request timestamps directly but rely on them as proof of the timestamped data's validity for legal, regulatory, or operational purposes.

4.6 Timestamp Policy and Practice Statement

This Timestamping Policy and Practices Statement outlines the minimum operational requirements for generating digital timestamps, ensuring compliance with the eIDAS Regulation (EU No. 910/2014) and relevant standards such as ETSI EN 319 421 and RFC 3161. Its primary objective is to ensure that timestamped data remains verifiable, legally recognized, and resistant to tampering over time.

Under eIDAS, a qualified timestamp provides legal certainty by proving that electronic data existed at a specific time, ensuring compliance with Article 41 of the regulation. One of its key features is high precision, guaranteeing that timestamp issuance occurs with an accuracy of one second or better.

The Timestamping Policy and Practices Statement is available as a public document on Incode's website: https://psc.incode.com/qtsp-legal-repository/

4.7 Conformance

The Incode TSA formally declares its conformance with this Policy/Statement across all issued timestamp tokens. Each timestamp token explicitly references this document through the identifier described in Section 5.2, ensuring traceability, consistency, and compliance with established standards.

As a Qualified Timestamp Authority, Incode operates within a regulated framework, adhering to industry best practices and legal requirements for trust services. To maintain its qualified status, Incode undergoes regular audits and compliance reviews conducted by relevant certification bodies and regulatory authorities. These evaluations verify that Incode's operations, security controls, and service delivery

continuously meet the obligations, policies, and technical standards outlined in this document.

Through continuous monitoring, security assessments, and adherence to regulatory frameworks (such as eIDAS, ETSI EN 319 421, and RFC 3161), Incode ensures that its timestamping services remain reliable, secure, and legally recognized.

5. Timestamp Policy

5.1 General requirements

The Timestamp Policy establishes the principles, operational framework, and security requirements governing the issuance, management, and validation of timestamps by Incode as a TSA. This policy ensures that timestamps provide irrefutable proof of the existence of electronic data at a specific point in time, maintaining compliance with ETSI EN 319 421, RFC 3161 and other applicable regulations.

5.2 Document name and identification

This document is identified by an Object Identifier (OID).

The OID for this Timestamp Policy is **1.3.6.1.4.1.22635891.1.3.1**, assigned in accordance with the regulations of the National Digital Signature Certification Center and following the IANA standard numbering format:

1.3.6.1.4.1.[EnterpriseNumber].[TypeCA].[codeTSA].[codeTSAPS]

Where:

- EnterpriseNumber identifier = 22635891.
- TypeCA identifier = 1 (public).
- QTSP codeTSA identifier = 3.
- codeTSAPS identifier = 1.

This structure ensures unique and standardized identification of the Certification Policy within the digital signature framework.

Document name: QTSP Timestamp Policy / Statement.

5.3 Users and applicability

The user community of Incode's timestamping service includes both natural and legal persons, categorized as subscribers and relying parties. Subscribers are subject to a contractual agreement with Incode to access the timestamping service. Incode does not offer a public timestamping service.

The timestamping service provided by Incode applies to any scenario where it is necessary to prove that electronic data existed at a specific point in time and has remained unaltered since then.

6. Policies and Practices

6.1 Risk Assessment

Incode conducts risk assessments for its TSA service to identify, evaluate, and mitigate risks that could impact the security, reliability, and integrity of its timestamping service. This assessment ensures compliance with ETSI EN 319 421, ETSI EN 319 401, and other applicable regulatory requirements while maintaining trust in the timestamping process.

Incode's risk assessment covers cryptographic risks, time source integrity, system availability, and downtime risks, among others. Additionally, it includes the development of a security plan and strategy to manage, control, mitigate, and eliminate risks effectively

6.2 Trust Service Provider Practice Statement

Incode defines a Timestamp Policy that establishes a comprehensive set of policies and operational practices aligned with ETSI EN 319 401, ETSI EN 319 421, and the eIDAS Regulation. These policies are formally approved by management and are published and communicated to relevant stakeholders and relying parties.

The TSA Management and Operational Practices are formally described in Section 7 of this policy, ensuring that the Incode TSA operates in a structured, transparent, and compliant manner.

The TSA Policy is made available to subscribers and relying parties through Incode's website at https://psc.incode.com/qtsp-legal-repository/.

6.2.1 Valid hashing algorithms

Incode TSA use cryptographically secure hashing algorithms that comply with ETSI EN 319 421 and other applicable regulations to ensure the integrity and authenticity of timestamped data. The selected hashing algorithms must meet industry standards for collision resistance, preimage resistance, and second-preimage resistance to prevent tampering or forgery of timestamps.

The following cryptographic hash functions are approved for use in the timestamping service:

- SHA-256
- SHA-384
- SHA-512

6.2.2 Accuracy of the time

Incode ensures that the time used for generating timestamps maintains an accuracy of within ±1 second relative to UTC. The time signal is provided by a Stratum-1 national time authority.

Incode maintains this accuracy under all operating conditions, including peak load scenarios, network latency variations, and system failures.

6.2.3 Limitations on the use of the service

No limitations have been declared.

6.2.4 Suscribers obligations

Subscribers of the timestamping service provided by Incode are required to comply with the obligations set forth in this policy to ensure the secure and proper use of timestamps. These obligations include:

- The subscriber must adhere to the requirements outlined in this Timestamp Policy, as well as any additional terms specified in the contractual agreement with the TSA.
- The subscriber must use timestamps only for their intended and legally permitted purposes.
- The subscriber is responsible for ensuring that the data submitted for timestamping is accurate, complete, and has not been tampered with prior to submission.
- The subscriber must ensure that timestamped data is properly stored and maintained to prevent unauthorized modifications after issuance.
- The subscriber is responsible for validating issued timestamps to ensure their authenticity, integrity, and compliance with relevant standards.
- The subscriber must use approved verification mechanisms to confirm the validity of timestamps received from the TSA.
- If any discrepancies or inconsistencies are detected, the subscriber must report them to the TSA immediately.
- If the subscriber becomes aware of any security breaches, unauthorized use, or potential compromise related to the timestamping service, they must promptly notify the TSA.
- The subscriber must cooperate with the TSA in investigating and resolving security-related incidents.

- The subscriber is responsible for ensuring that timestamped records are stored for the required duration in accordance with applicable regulations and business needs.
- The TSA is not responsible for retaining timestamped data beyond the issued timestamp record itself.

6.2.5 Relying parties obligations

To ensure the proper use and trustworthiness of timestamps issued by Incode, relying parties must comply with the following obligations:

- Relying parties must validate timestamps before trusting them, using appropriate cryptographic verification mechanisms.
- Verification should confirm that:
  - The timestamp was issued by Incode's Timestamping Authority (TSA).
  - The timestamp is cryptographically intact and has not been altered.
  - The TSA's digital signature is valid and has not been revoked.
- Relying parties should use trusted timestamp validation tools or services to ensure compliance with industry standards and regulations.
- Relying parties must adhere to the terms and conditions outlined in this Timestamp Policy.

6.2.6 Timestamp verification

Relying parties must validate a timestamp by confirming that:

- It was issued by Incode TSA.
- The timestamp is cryptographically valid, ensuring that the associated data has not been altered since the time of stamping.
- The digital signature of Incode TSA is valid, unexpired, and not revoked.
- The timestamp adheres to ETSI EN 319 421 and any applicable regulations.

6.2.6.1 Long-Term timestamp verification

Long-term verification of timestamps ensures that timestamped data remains valid, trustworthy, and legally admissible over extended periods and according to Annex D of ETSI EN 319 421 timestamp verification can still be performed after TSA certificate expiration, considering:

1. The TSA or TSU private keys have not been compromised.
2. Hash functions and digital signatures algorithms have not become vulnerable.
3. Signature key sizes are still supported by this Policy and CPS.

6.2.7 Applicable Law

Any claim related to Incode TSA or its issued timestamps should be addressed as stated in Section 9.13 (Dispute Resolution) of the CPS.

6.2.8 Availavility

Incode is committed to providing a highly available and reliable timestamping service to ensure uninterrupted access for subscribers and relying parties. Incode TSA implements robust infrastructure, redundancy mechanisms, and failover strategies to maintain operational continuity and minimize downtime.

Incode TSA is deploy to meet the following availability objectives:

- Availability rate of at least 99.9%, except during scheduled maintenance or unforeseen incidents.
- Timestamp requests shall be processed within defined performance benchmarks, ensuring minimal latency.
- In the event of a system failure, the failover mechanism should be triggered.

6.3 Terms and Conditions

The General Terms and Conditions outline the scope, limitations, and obligations associated with the Timestamping Service provided by Incode.

This policy defines the limitations of the timestamping service, as well as the responsibilities and obligations of:

- Incode TSA providing the service.
- Subscribers who request timestamps.
- Relying parties who validate and depend on issued timestamps.

While this policy establishes the general operational and legal framework, additional terms and conditions may be specified in contractual agreements required for the establishment and ongoing provision of the service.

6.4 Information Security Policy

As part of its Information Security Management System (ISMS), Incode has developed and implemented a comprehensive Information Security Policy. This policy integrates all security policies, procedures, standards, and guidelines applied by Incode to secure its trusted services.

Some of the key security controls applicable to the TSA are described in CPS sections:

- Section 5 – Management, Operational, and Physical Controls
- Section 6 – Technical Security Controls
- Section 8 – Compliance Audits and Other Assessments

The Information Security Policy has been formally approved by Incode Management and has been acknowledged and communicated to all employees.

6.5 TSA Obligations

6.5.1General

No estipulation

6.5.2 TSA obligations towards subscribers

Incode TSA is responsible for ensuring the secure, reliable, and compliant operation of its timestamping service. The following obligations define the TSA's commitments toward subscribers, ensuring the trustworthiness, integrity, and legal reliability of issued timestamps.

- Issue timestamps in compliance with this Policy and with ETSI EN 319 421 and applicable legal frameworks.
- Ensure that timestamps are digitally signed and tamper-proof, using cryptographic mechanisms that comply with current security standards.
- Synchronize timestamps with a trusted Coordinated Universal Time (UTC) source, maintaining an accuracy of ±1 second.
- Ensure high availability of the timestamping service, implementing failover mechanisms and disaster recovery plans to minimize disruptions.
- Provide advance notice of any planned maintenance or significant service changes that may impact subscribers.
- Undergo regular audits to demonstrate compliance with ETSI EN 319 421, ETSI EN 319 401, eIDAS, and other applicable standards.
- Ensure that policies, security controls, and timestamping operations are transparent and verifiable by regulatory bodies.

6.6 Information for Relying Parties

Relying parties of timestamps issued by Incode TSA are obligated to properly verify the timestamps before relying on them. This includes, but is not limited to:

- Verifying that the timestamp has been correctly signed by Incode TSA.
- Ensuring that the private key used to sign the timestamp was valid and had not been compromised at the time of issuance.

7. TSA Management and Operation

7.1 Introduction

Incode implements an Information Security Management System (ISMS) aligned with ISO 27001, ensuring the confidentiality, integrity, and availability of its TSA services. The ISMS includes a comprehensive set of security policies, procedures, and controls that govern the administration, management, and operation of the TSA. These policies define strict access controls, risk management measures, and compliance frameworks to protect timestamping operations.

Regular audits and security assessments are conducted to maintain regulatory conformance and operational security. Through this ISMS, Incode ensures that its TSA operates securely, transparently, and in full compliance with ETSI EN 319 421 and applicable laws.

7.2 Internal organization

Incode TSA is a service provided by Incode Czech Republic, a legally recognized entity incorporated in Czechia, operating in compliance with the eIDAS Regulation and Czech national laws. Incode TSA implements an ISMS to ensure the confidentiality, integrity, and availability of its timestamping services.

Incode TSA employs qualified personnel who must comply with Section 7.3 of this policy and possess expertise in cryptographic security, regulatory compliance, and risk management, ensuring the proper administration and operation of the service.

Additionally, Incode TSA is subject to periodic audits and security assessments to ensure continuous compliance with applicable laws and regulatory standards.

These measures ensure that Incode TSA provides reliable, secure, and legally valid timestamps for digital transactions and regulatory use.

7.3 Personnel security

To ensure the security, integrity, and trustworthiness of its TSA, Incode implements strict personnel security policies in compliance with ETSI EN 319 421, ETSI EN 319 401, and ISO/IEC 27001. These measures ensure that only authorized, qualified, and trustworthy personnel have access to TSA operations and sensitive cryptographic materials.

Details of the personnel security controls implemented by Incode can be found in Section 5.3 of the CPS, which, among other things, describes:

1. Bakcground check procedures
2. Competence, experience and other requierements to operate the CA and TSA.

Incode has well-defined job descriptions for trusted roles responsible for the administration, management, and operation of the CA and TSA. These roles are assigned based on strict security and compliance requirements, ensuring that only authorized personnel perform critical tasks. Additionally, the framework enforces a clear separation of duties, minimizing the risk of conflicts of interest and enhancing the overall integrity and security of trust services.

7.4 Asset management

Incode implements an Asset Management Policy as a comprehensive framework for managing the lifecycle of organizational assets, particularly storage media. This policy establishes clear guidelines, procedures, and responsibilities for the protection, control, and disposal of assets to ensure compliance with information security standards.

The Asset Management Policy defines the principles to be followed throughout the entire asset lifecycle—from issuance and allocation when an employee joins the company to retirement when the asset becomes non-functional or upon the employee's departure.

As a Qualified Trust Service Provider (QTSP), Incode considers this policy essential for maintaining the confidentiality, integrity, and availability of data. It also ensures the secure disposal of storage media to prevent unauthorized access or data breaches.

7.5 Access control

Incode limits unauthorized access to systems and information by establishing, maintaining, monitoring, and disabling accounts with appropriate levels of authorization and permissions.

Incode identifies system owners and assigns system administrators to manage accounts on systems used in Incode's business. Incode:

- Identifies sensitive systems;
- Assigns system owners and system administrators;
- Establishes conditions for group and role membership (as applicable);
- Specifies authorized users of the information system, group and role membership, and access authorizations (i.e. account privileges) and other attributes (as required) for each account;
- Requires approval by system owner to create information system accounts if the access is outside of their standard job description;
- Creates, enables, modifies, disables, and removes information system accounts in accordance with this procedure;
- Monitors the use of information system accounts;

7.6 Cryptographic controls

7.6.1 General

Cryptographic key generation in Incode TSA follows strict security protocols to ensure the integrity and confidentiality of cryptographic operations. All cryptographic keys are generated within a FIPS 140-2/3 Level 3 or Common Criteria EAL4+ certified HSM, ensuring compliance with industry standards for secure key management. The key generation process is designed to maintain high entropy, preventing any predictability or weaknesses that could lead to cryptographic compromise. Key sizes are carefully selected to align with recommended security strengths, utilizing RSA 4096-bit for long-term security and ECC P-256/P-384 for optimized performance with strong cryptographic resistance. By implementing these best practices, Incode TSA ensures that all cryptographic operations are conducted in a highly secure and compliant environment.

7.6.2 TSU Key Generation

The TSU within Incode TSA follows a strict and secure key generation process to ensure the integrity, authenticity, and non-repudiation of timestamps. The TSU signing key is a critical cryptographic asset and must be managed in compliance with ETSI EN 319 421, RFC 3161, and NIST SP 800-57 standards.

Incode secure generation process, ensures:

- The TSU signing key is generated inside a FIPS 140-2/3 Level 3 or higher certified HSM to prevent unauthorized access.
- The key generation process ensures sufficient entropy, minimizing predictability and cryptographic vulnerabilities.
- The generation is performed by trusted roles to ensure accountability and security.
- The TSU key pair follows best practices, using RSA 4096-bit with SHA-256/SHA-512 for long-term security.

7.6.3 TSU Private Key Protection

The TSU private key is generated, stored, and used exclusively within a FIPS 140-2/3 Level 3 certified HSM, ensuring physical and logical isolation from unauthorized access. The key is never exported from the HSM, and built-in encryption mechanisms protect it from extraction, tampering, or misuse.

Strict Role-Based Access Control (RBAC) and multi-factor authentication (MFA) limit key management operations to authorized Crypto Officers, enforcing a segregation of duties policy.

The private key is used solely for timestamp signing operations, ensuring non-repudiation and compliance with RFC 3161, reinforcing trust in the integrity of issued timestamps.

7.6.4 Public Key Certificate

The TSU public key certificate is publicly accessible through a trusted public key certificate, allowing relying parties to verify timestamp signatures and ensure their authenticity. It is distributed via the TSA's certificate repository, ensuring that external systems and auditors can securely retrieve and validate issued timestamps.

Additionally, the certificate is embedded in timestamp responses (TSRs) in accordance with RFC 3161, facilitating seamless and automated verification by relying parties, thereby strengthening the trust and integrity of the timestamping process.

7.6.5 Rekeying TSU's key

Incode does not implement rekeying processes. If certificates, algorithms, or key sizes are deemed vulnerable, a new key pair will be generated and used to issue a new certificate.

7.6.6 Life cycle management of signing cryptographic hardware

The procurement, deployment, and decommissioning of CloudHSMs used by Incode must follow strict security protocols to ensure compliance with industry standards and protect cryptographic operations. CloudHSM services are provisioned from trusted cloud providers that adhere to FIPS 140-2/3 Level 3 certifications and enforce strong access controls.

The secure deployment process ensures that only authorized personnel can initialize and configure the HSM, with multi-factor authentication (MFA) and role-based access control (RBAC) enforcing strict governance. Before activation, the firmware and security configurations of the CloudHSM instance must be verified to align with Incode's security policies, ensuring secure key generation, storage, and access management.

Throughout its operational lifecycle, CloudHSM activity is continuously monitored, with logging and audit mechanisms in place to track cryptographic operations. When a CloudHSM reaches end-of-life, the associated signing keys must be permanently deleted, ensuring they cannot be recovered.

The CloudHSM instance is then decommissioned securely within the cloud provider's infrastructure, with a final compliance audit conducted to verify proper key destruction and service termination..

7.6.7 End of TSU key cycle

The TSU key lifecycle follows a structured process to ensure security, compliance, and continuity in timestamping operations. TSU signing keys are assigned a validity period based on cryptographic best practices and regulatory requirements. Before expiration, a new key pair is generated, and a new TSU certificate is issued by Incode trusted CA to ensure seamless transition without disrupting timestamp validation.

If a TSU key is compromised or reaches its end of life, it is immediately revoked to prevent further use, and a CRL or OCSP response is published to notify relying parties. The revoked key is then deactivated within the HSM, ensuring it can no longer be used for signing.

Once decommissioned, the private key is permanently erased using cryptographic erasure techniques, ensuring it cannot be recovered or reused.

7.7 Timestamping

7.7.1 Timestamp issuance

Timestamp issuance process from Incode TSA is designed to comply with ETSI EN 319 422, ensuring secure, accurate, and verifiable time-stamp generation. All issued time-stamps conform to the time-stamp profile defined in ETSI standards and are generated through secure and tamper-resistant processes.

To guarantee time accuracy, the timestamp includes a correct and traceable time value, synchronized with UTC through a recognized UTC(k) laboratory. These laboratories, officially recognized by the BIPM, ensure that timestamps maintain scientifically verifiable accuracy.

In the event that the TSA's clock drifts beyond the allowed accuracy, timestamps are not issued until synchronization is restored and each timestamp is digitally signed using a dedicated TSU signing key, generated exclusively for this purpose, ensuring cryptographic integrity and non-repudiation.

Furthermore, the timestamp generation system rejects any timestamp issuance attempts if the TSU private key has expired or is no longer valid.

7.7.2 Clock synchronization with UTC

Ensuring precise clock synchronization with UTC is fundamental for Incode TSA to generate trusted and verifiable timestamps. Incode TSA follows ETSI EN 319 421, ETSI EN 319 422, and ITU-R TF.460-6 standards to maintain accurate time references for all issued timestamps.

- Incode TSA time source is traceable to a recognized UTC(k) laboratory, which is part of the global Bureau International des Poids et Mesures network.
- The TSA ensures its internal clock remains synchronized with UTC within the accuracy defined by its timestamp policy.
- Incode ensures that the time used for generating timestamps maintains an accuracy of within ±1 second relative to UTC.
- The TSA continuously monitors its clock for deviations from UTC.
- If the system detects that the clock has drifted beyond the allowed accuracy, timestamp issuance is immediately paused until synchronization is restored.

7.8 Physical and environmental security

Incode TSA operations are conducted within a protected physical environment designed to prevent and detect unauthorized access, use, or disclosure of sensitive information. This environment complies with QTSP security requirements and QTSP testing standards.

The security requirements are based in part on physical layer security measures, which include:

- Perimeter protection, such as fences, locked doors, and controlled access points, ensuring that only authorized individuals can proceed to the next security layer.
- Each layer provides increasingly restricted access, offering greater physical security against unauthorized entry.
- The security structure follows a layered approach, where each inner layer is fully encapsulated within the outer layer, creating a progressive security model.

7.8.1 Physical access

Incode TSA servers are housed in a controlled environment with restricted access, enforced through individual access rights. Incode TSA signing system operates on dedicated servers, and the private key is securely stored when not in use to ensure its protection and integrity.

7.8.2 Air condition and power supply

- Servers providing online services are operated in a properly conditioned environment, and do not restart except for essential maintenance.
- Servers of Incode TSA system are protected by UPS system and backup generator in case of mains power failure.

7.8.3 Contact with water

The location of Incode TSA system equipment is selected appropriately, and a preventive plan is developed to prevent water and flood from entering the system.

7.8.4 Fire protection and prevention

The data centers housing Incode TSA infrastructure, in compliance with the SOC 2 report, have fire protection policies and procedures in place to ensure that infrastructure equipment remains protected in the event of a fire incident.

7.8.5 Storage media

All media containing production software and data, audit records, archives, or backup information is stored within Incode's AWS account, with appropriate logical access controls in place to restrict access to authorized personnel. Additionally, the data is protected by backup policies to prevent data loss or damage.

7.8.6 Garbage treatment and destruction

Waste management at data center facilities is subject to the policies and regulations established by AWS.

Regarding waste management within Incode's controlled procedures, particularly those related to media handling, Incode follows a Media Handling Policy that defines the sanitization procedures required for physical and electronic media. These procedures ensure that media is securely destroyed, preventing any exposure or reuse of the stored information.

7.8.7 Remote backup

Incode TSA processes and systems have automated backup mechanisms that enable immediate recovery points in the event of a failure. These backups are securely stored with redundancy across the data processing regions where Incode operates within the AWS cloud, in compliance with its backup policy.

7.9 Operation security

Incode TSA ensures the integrity, security, and reliability of its timestamping services through strict operational security controls. Security is embedded from design, with rigorous change control, malware protection, and access management to prevent unauthorized modifications. Role-based access control and multi-factor authentication (MFA) safeguard administrative functions, while timely patching and continuous monitoring ensure system integrity. Our configuration management enforces security baselines with automated compliance checks and real-time threat detection.

Incode TSA continuously monitors capacity demands to ensure optimal system performance and prevent resource shortages. Projections of future capacity requirements are made based on usage trends and growth forecasts. Scaling is managed through auto-scaling cloud functionality, allowing Incode TSA to allocate resources dynamically according to service demand. This approach ensures the availability, reliability, and efficiency of services while mitigating potential disruptions.

7.10 Network Security Control

Incode TSA operate within a secured network, following security policies and standard compliance documents to prevent unauthorized access, tampering, and attacks on the service.

To ensure reliability and authentication, all communications and critical information are protected using point-to-point encryption and digital signatures for validation.

Additionally, all other TSA systems are safeguarded through:

- Firewalls to restrict unauthorized access.
- Intrusion Detection and Prevention Systems (IDS/IPS) to monitor and mitigate threats.
- The removal of unnecessary services to minimize vulnerabilities.

7.11 Incident Management

Incode has implemented an Information Security Incidents Procedure designed to facilitate the reporting of security incidents, potential vulnerabilities, and behaviors that may compromise information systems. This procedure outlines the methods for

reporting, monitoring, and responding to incidents to ensure a structured and effective resolution process.

The procedure includes mandatory notifications to relevant authorities in the event of security incidents that could impact the trustworthiness of Incode's trusted services. Additionally, subscribers and relying parties are informed as necessary to maintain transparency and trust.

Employees play a critical role in the Information Security Management System by adhering to that policy and actively reporting incidents. All reported cases are tracked, analyzed, and addressed through corrective and preventive actions, ensuring that measures are implemented to prevent recurrence and strengthen overall security.

7.12 Collection of evidence

As part of this Policy, Incode ensures that all timestamping operations are auditable and verifiable by implementing strict evidence collection procedures. This ensures compliance with eIDAS legal and regulatory framework while maintaining the integrity, authenticity, and reliability of issued timestamps.

To support the validity of each issued timestamp, the following data is systematically recorded:

- Events related to TSA and TSU keys and certificates.

7.13 Business Continuity Management

Incode has established business continuity management procedures for scenarios involving potential compromise of its TSA private key or loss of time synchronization with the UTC reference source.

7.13.1 Response to TSA Private Key Compromise

If there is any suspicion of compromise or unauthorized access to the TSA's private key or its TSUs, Incode will take immediate action to protect the security and trust of its timestamping service. The response includes:

- Following the procedures outlined in Section 5.7 of the CPS to assess, confirm, and mitigate any potential key compromise.
- Ceasing the issuance of timestamps until a new cryptographic key is generated, securely stored, and validated to maintain trust in the service.

- Revoking and replacing the compromised TSA certificate and notifying subscribers, relying parties, and relevant authorities of the security incident.
- Conducting forensic analysis to determine the root cause, scope, and impact of the compromise.
- Implementing additional security measures to prevent future incidents, such as stricter key management controls, enhanced monitoring, and additional authentication layers.

7.13.2 Automated Time Synchronization Monitoring and Response

Incode TSA relies on highly accurate time sources to ensure that timestamps comply with regulatory requirements, particularly maintaining a precision of ±1 second with UTC. To guarantee this accuracy:

- Automated monitoring mechanisms continuously verify synchronization with UTC reference sources.
- If loss of synchronization is detected or the precision threshold of ±1 second cannot be met, the TSA will automatically suspend timestamp issuance until synchronization is restored.
- Alerting mechanisms notify system administrators of any deviation, allowing for immediate corrective action to restore service integrity.

7.13.3. Notification to Relevant Authorities

In any of the above scenarios, Incode will promptly notify relevant regulatory authorities in compliance with its Incident Management Policy and applicable legal obligations. The notification process includes:

- Providing detailed reports on the nature of the incident, potential impact, and mitigation steps taken.
- Engaging with regulatory bodies, subscribers, and relying parties to ensure transparency and maintain trust in the service.
- Executing a controlled recovery plan to re-establish secure timestamp issuance while ensuring compliance relevant regulation.

7.14 TSA termination and termination plans

In the event that Incode TSA is terminated, Incode will implement a structured termination plan to ensure the controlled and secure discontinuation of its trust services, minimizing disruptions for relying parties and ensuring compliance with applicable legal and regulatory requirements.

7.14.1 Revocation of Unexpired Certificates

Upon termination, Incode will:

- Revoke all active TSA certificates to prevent any unauthorized use of timestamps after the service has been discontinued.
- Notify subscribers and relying parties in advance about the revocation schedule, ensuring they take necessary actions to transition to alternative services.
- Publish CRLs or update the OCSP responders to reflect the revocation status.
- Ensure timestamping records remain accessible for the required retention period to support legal evidence and verification needs.

7.14.2 Compliance with CPS and Regulatory Standards

The termination of Incode TSA follows the procedures described in Section 5.8 of Incode CPS, which outlines the required steps for the orderly termination of a CA or RA. These steps include:

- Regulatory Notifications: Informing supervisory bodies, accreditation authorities, and relevant regulatory entities about the termination.
- User and Partner Communication: Notifying all stakeholders, including subscribers, relying parties, and integrators, about the transition plan and timeline.
- Secure Key and Data Disposal: Implementing secure decommissioning procedures for cryptographic keys, ensuring that all TSA private keys are properly destroyed in compliance with cryptographic best practices to prevent misuse.

7.14.3 Data Retention and Legal Obligations

Even after the termination of services, Incode will:

- Ensure timestamp records remain accessible for verification purposes within the legally required retention period.
- Maintain audit logs and records securely, ensuring they can be used for dispute resolution or compliance audits.
- Provide an official statement detailing the termination and its impact, ensuring transparency and clarity for affected parties.

8. Additional requirements for qualified electronic timestamps as per Regulation (EU) No 910/2014

When a timestamp claims to be a qualified timestamp, relying parties are expected to verify whether a timestamp and its issuing TSU are qualified by consulting a Trusted List. If the public key of the TSU appears in the Trusted List and is associated with a qualified time-stamping service, the timestamps it issues can be considered qualified.

In cases where a Timestamping Authority (TSA) operates multiple TSUs, the public key of the TSA may be listed in the Trusted List under ETSI TS 119 612. If the TSA is recognized for providing qualified time-stamping services, and a TSU is properly identified within its certificate, then the timestamps issued by that TSU are also qualified. Additionally, the presence of the qcStatement "esi4-qtstStatement-1", as defined in ETSI EN 319 422, clause 9.1, serves as an indication that a timestamp is being claimed as a qualified electronic timestamp.

Incode PSC