incode psc

Remote Signature Policy Statement

Version	Modified by	Modifications made	Date modified
1.0	LV	Content	20/04/2025

Tabla de contenido

1 Introduction

This document outlines the principles and operational guidelines followed by Incode Czech Republic s.r.o. (hereinafter referred to as Incode) in the provision of its remote signature service.

It also describes the responsibilities and actions required from the end user in relation to the issuance and management of the qualified electronic certificate associated with the service.

The service is primarily intended for the electronic signing of documents using qualified certificates issued by Incode.

As part of the signature process, the qualified certificate is securely stored in a Qualified Signature Creation Device (QSCD), which remains under the exclusive control of Incode, ensuring compliance with applicable regulatory and security requirements.

The statutory requirements in respect of the Service are defined in:

- Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended;
- Act of the Czech Republic No. 297/2016 Coll., on trust services for electronic transactions;
- Legislation concerning personal data protection in compliance with Regulation (EU) no 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.1 Overview

This document named as **Remote Signature Policy Statement**, is elaborate by Incode which defines the governance policies in the provision of the service of remote signature.

This document serves as a statement of obligations undertaken by the QTSP for customers using its remote electronic signature service. It is important to note that this document does not constitute a legal agreement between Incode and its customers but rather provides:

- Technical, business, and legal requirements for the public key infrastructure (PKI) service provided by Incode.

- Authentication policies and procedures for customers utilizing the electronic authentication service offered by the QTSP, as well as the rights and obligations of customers participating in the service.
- The level of assurance associated with a digital certificate issued by the QTSP and the reliability of digital signatures made using such certificates.
- Information for the relying party regarding the level of trust and assurance provided by a QTSP-issued certificate.

This document exclusively governs the provision of remote electronic signature and does not extend to other services provided by Incode.

1.2 Document name and identification

Document name: Remote Signature Policy Statement.

Supported OIDs: 0.4.0.19431.2.1.2 (eu-advanced-x509, AdES based on X.509 certificates); and

0.4.0.19431.1.1.3 (EU SSASC policy) - in case of storage signing keys in QSCD

1.2.1 Signature creation policy

A single signature creation policy is supported at any given time within the service. The applied version of the signature creation policy is determined by the time when a particular electronic signature was created.

1.2.2 Supported signature formats and baselines

1.2.2.1 Baselines

B-B	A minimal and standardized profile ensuring interoperability without including a Timestamp
B-T	Provides the generation and inclusion of a timestamp token for an existing signature, proving that the signature itself actually existed at a certain date and time.
B-LT	Provides the incorporation of timestamp token and information about the revocation status of the signing certificate.
B-LTA	Provides the incorporation of timestamp tokens that allow validation of the signature long time after its generation. This level aims to tackle the long-term availability and integrity of the validation material.

1.2.2.2 Formats

1.2.2.2.1 PAdES

PAdES (PDF Advanced Electronic Signature) is a standard that defines how to embed electronic signatures in PDF documents in a secure and legally compliant way. Based on ETSI and aligned with eIDAS, PAdES ensures the authenticity, integrity, and long-term validity of signed PDFs. It supports various levels, from basic signatures to timestamped and fully validated signatures for long-term archiving.

Incode support the use of visible and invisible versions of the signature.

Visible signature could be place in the document in three different ways:

1. Text only
2. Image only
3. Text and image

1.3 PKI Participants

1.3.1 Service provider

Incode Czech Republic s.r.o. as the qualified trust service provider

1.3.2 Relying parties

Any entity relying on electronic signature create using the Incode remote signature service.

1.3.3 Other participants

Other participating parties are investigative, prosecuting and adjudicating bodies, supervisory bodies and other bodies recognized as such by current legislation.

1.4 Service usage

1.4.1 Appropiate service uses

Remote signature services provided under this policy are intended to support electronic signing operations in which the signatory's private key is securely managed, and the signing operation is performed remotely by the user through secure authentication mechanisms to the benefit of the signer and/or the third parties involved in compliance with the current legislation.

1.4.2 Prohibited service uses

Remote signature under this policy may not be used against the approved usses described in section 1.4.1 or contrary lo law. It also may not be used for:

1. Use by Unauthorized or Unverified Individuals
2. Automated or Delegated Signature without Explicit Authorization
3. Use Outside the Defined Scope of Service

1.5 Policy administration

1.5.1 Organization Responsible for the Policy

This Policy its administered by Incode Czech Republic s.r.o.

1.5.2 Contact person

The contact person of Incode as in respect of this Policy is the CA Manager. The contact information provided in chapter 2.2 applies.

1.5.3 Person determinin suitability for the policy

CA Director is the sole person responsible for making decisions about compliance of the procedures of Incode Czech Republic, s.r.o. as established in this document.

A review of the procedures established in this document will be conducted at least once a year. If necessary, updates will be made, and any changes along with the updated statement will be published on the designated portal provided by Incode for this purpose.

As part of the annual reviews and adaptation of applicable procedures and policies, the CA Director is responsible for determining the applicability of the Remote Signature Police Statement and its associated policies.

1.6 Definitions and Abbreviations

1.6.1 Definitions

Terms	Explain
Init code	QR code or URL link used to initializiate the service for specific client
Signer identity	Identity from the signer obtain through a remote identity verification process provided by Incode.
Classified Information Protection Act	Act of the Czech Republic no. 412/2005 Coll., on the protection of classified information and security eligibility
Electronic signature	Advanced Electronic Signature or Qualified Electronic Signature provided under trust service legislation.
Remote Electronic Signature	Electronic signature created using private key stored in a device operated, managed and secured by Incode. This private key is under sole control of the client.
Trust Service / Qualified Trust Service	Defined by trust services legislation.
Supervisory body	The body supervising qualified trust service providers.

1.6.2 Acronyms

Symbol	Full name
AdES	Advanced electronic Signature
CR	Czech Republic
eIDAS	REGULATION (EU) no 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended
EN	European Standard, a type of ETSI standard
ETSI	European Telecommunications Standards Institute, a European standardization institute for information and communication technologies
HSM	Hardwate Security Module
OID	Object Identifier
PAdES	PDF Advanced Electronic Signatures
XAdES	XML Advanced Electronic Signatures

2 Responsibility for publication and storage

2.1 Storage

Incode is responsible for maintaining avalability for the repositories where the information of their policies and public information it's been published.

2.2 Publication of certification information

The registered office of Incode Czech Republic, s.r.o., for purposes of obtaining information about its operations, is as follows:

- Pujmanové 1753/10a, Nusle, 140 00 Prague 4
- https://psc.incode.com/eu/
- tsp@incode.com

Electronic address for contact between general public and Incode Czech Republic s.r.o. info@incode.com.

Data box of Incode Czech Republic s.r.o. ID is 76gmkd8

2.3 Information disclosure frequency

Incode publishes information as follows:

- Policy of the service. After a new version is approved and issued.

2.4 Acces controls on repositories

Incode does not require authentication for third-party access to this Policy through the designated online disclosure address.

3 Identification and Authentication

3.1 Initial identity verification

3.1.1 How to prove possession of secret key

All private keys are generated internally, within the signature process, by Incode Issuer CAs and securely stored in a Hardware Security Module (HSM).

If the Issuer CA or RA does not generate the Subject's key pair, the CA or RA must verify:

a) The electronic signature included in the PKCS #10 Certificate Signing Request (CSR) to ensure it corresponds to the public key of the requester.
b) The integrity of the signed data within the CSR.

3.1.2 Identification and authentication for individual subjects

The authentication of an individual's identity follows a remote identity verification process to ensure security, compliance, and efficiency. The process typically involves the following steps:

1. Initiation of Certificate Request

- The applicant initiates the process to request a certificate or complete a remote signature transaction. The validity period may vary depending on the specific process and requirements.

2. Submission of Identity Documents

- The applicant must provide a government-issued identity document (e.g., passport, national ID, driver's license, visa).
- The document is captured using a mobile device through Incode's secure web portal or mobile application.
- Optical Character Recognition (OCR) technology extracts and validates the document details.
    - System collects identifying details such as full name, expiration date, issuance country and other relevant information from the provided documents.
- Advanced document authenticity checks (e.g., watermark detection, hologram verification, MRZ scanning) are performed to prevent fraud.

3. Remote Liveness & Biometric Verification

- The applicant must complete a liveness detection check including the following methods:
    - Selfie capture with AI-driven liveness passive detection.
    - Biometric matching between the selfie and the ID document photo.
- Incodes AI-based facial recognition technology ensures that the applicant is physically present and not using manipulated images or deepfakes.

4. Data Cross-Validation & Fraud Prevention Checks

- The extracted information is cross-checked against:
    - Government databases (if applicable).
    - Sanctions lists and watchlists (for AML/KYC compliance).
    - Previous verification attempts to detect anomalies or inconsistencies.

- The system flags potential identity fraud, duplicate identities, or suspicious behavior.

5. Certificate Issuance

- If the verification is successful a signatture certificate is issued with specific:
  - Defined validity period.
  - Restricted usage scope (e.g., a single transaction, single session, document signing).

5. Remote Signature

  - After the certificate has been issued and with the consent of the certificate holder, the presented documents are signed.

7. Expiration & Auto-Revocation

- The short-lived certificate automatically expires after its designated validity period.
- If suspicious activity is detected post-issuance, the certificate can be revoked immediately via Online Certificate Status Protocol (OCSP) responses.

3.2 Modification of data

There is no possibility for modification of data in the certificate after it has been issued. If data needs to be changed or the certificate holder requires a new certificate, the process described in section 3.1.2 must be followed.

4 Service Life-Cycle Operational Requirements

In the following sections, the remote signature Service Life-Cycle will be described in detail. Readers of the Policy will gain insights into the key processes, technical requirements, and compliance considerations at each stage of the service lifecycle.

4.1 Service activation

The service is activated when the user receives the Init Code from a third party and begins the identity verification process.

4.1.1 Enrollment process and responsabilities

Identity verification process must be carried out as defined in section 3.1.2 every time the user uses the remote signature service.

The user, among other things, is required to do the following:

- Get acquianted with this Policy and the CPS for issuing qualified certificates for remote electronic signatures.
- Use the service in compliance with section 1.4
- Provide true and complete information for setting up the service.
- Check whether data from submitted documents are correct and correspond to the requiered data.

Among other responsibilities, Incode is required to do the following:

- Inform the user the terms and conditions before starting the remote signing process.
- During the identity verification process validate all the validable data according to the submitted documents.
- Issue a signing certificate that contains correct data on the basis of the information provided by the user.
- Publish the certificates of issuing and root CAs

4.1.2 Conducts constituting certificate acceptance

The user confirms acceptance by:

- Implicit acceptance, which may occur if the subscriber uses the certificate for its intended purpose (e.g., signing a document).
- For remote digital signature processes, acceptance is confirmed before the signing process, so no further action is required.

4.2 Certificate Revocation and Suspension

4.2.1 Certificate Revocation

Certificate revocation is the permanent invalidation of a digital certificate before its expiration date. Once revoked, the certificate cannot be reinstated and must be replaced if necessary.

A digital certificate may be revoked for various security, compliance, or operational reasons, including:

1. Private Key Compromise – The private key associated with the certificate has been lost, stolen, or exposed, potentially leading to unauthorized use.
2. Unauthorized Key Usage – The private key is being used for purposes not permitted by the certificate's intended usage.
3. Cryptographic Weakness – The certificate's cryptographic algorithms or key lengths are no longer secure due to advances in cryptanalysis or newly discovered vulnerabilities.

4. Voluntary Certificate Revocation – The subscriber requests revocation, as they no longer require the certificate.
5. Subscriber's Private Key Lost or Misused – The subscriber loses control of their private key, making it necessary to revoke the certificate to prevent misuse.
6. Change in Subscriber Information – The subscriber's legal name, organization details, or other critical information changes, making the existing certificate invalid.
7. Falsified or Incorrect Information – The certificate was issued based on inaccurate, incomplete, or fraudulent information.
8. Violation of Terms & Policies – The subscriber has violated the Certificate Policy (CP), Certificate Practice Statement (CPS), or Service Agreement.
9. Certificate Misuse or Unauthorized Use – The certificate is used in ways that violate its intended purpose, potentially compromising security.
10. CA Determines a Risk to Security or Reputation – The Certification Authority (CA) or Qualified Trust Service Provider (QTSP) identifies the certificate as a potential threat to security, reliability, or reputation.
11. Involvement in Fraud, Cybercrime, or Malicious Activity – The certificate is linked to fraudulent activities, phishing attacks, hacking, or other illegal actions.
12. Subscriber Does Not Comply with This Policy – The subscriber fails to meet the ongoing requirements outlined in the CPS or applicable regulations.
13. Subscriber Being an Individual is Dead or Declared Missing – If the subscriber has passed away or has been legally declared missing by a court, their certificate must be revoked.

4.2.1.1 Who can request the revocation?

A digital certificate revocation request can be submitted by the following authorized entities:

1. Certificate key owner.
2. CA, Issuer CA or RA.
3. Government agency, court, or regulatory authority.
4. Employer or organization.

4.2.1.2 Procedure for requesting revocation of certificate

Standard Revocation Request

- The user must send an email requesting revocation.
- The email must be digitally signed using the private key of the certificate (provided the certificate is still valid and has not expired).
- This ensures authenticity and prevents unauthorized revocation requests.

Emergency Revocation Request

- If the user cannot send a digitally signed email (e.g., due to key compromise or loss), the revocation request can be reported directly to the RA or Issuer CA of the QTSP.
- In such cases, alternative identity verification procedures must be followed to confirm the legitimacy of the request.

4.2.1.3 Revocation request grace period

If there is suspicion of key compromise or any other revocation reason outlined in Section 4.2.1, the user must submit a revocation request as soon as possible within a reasonable timeframe. Delays in submitting the request increase the risk of unauthorized use of the compromised key.

The CA is not responsible for any damages resulting from the illicit or unauthorized use of the subscriber's private key before the certificate is revoked. The subscriber is solely responsible for protecting their private key and reporting any suspected compromise promptly.

4.3 Use of the service

Incode provides the service for the remote creation of electronic signatures. Documents to be signed are sent by third parties, and the procedure is as follows:

1. The third party creates a signing flow that includes the document to be signed and sent the Init Code to the user.
2. User access the flow using the Init Code provided by the third party and completes de identity verification process.
3. User review the content of the document to be signed presented in application.
4. If the user has decided to consent the content of the document to be sign he press the button "sign".
5. User need to check the checkboxes present in the flow to express consent on the process, the issuance of a qualified certificate and the signature of the document with the issued certificate.
6. Once all checkboxes are marked user press "Continue" button.
7. CA issue the qualified certificate for the electronic signature which will be stored in a secure cryptographic device.
8. The remote electronic signature is completed using the private key created in step 7.

5 Management, Operational, and Physical Controls

5.1 Physical level control

QTSP and RA 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.

The minimum physical security level required by the QTSP and RA is determined by the highest level of certificate security they enforce.

5.1.1 Physical access

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

5.1.2 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 QTSP system are protected by UPS system and backup generator in case of mains power failure.

5.1.3 Contact with water

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

5.1.4 Fire protection and prevention

The data centers housing Incode's CA 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.

5.1.5 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.

5.1.6 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.

5.1.7 Remote backup

Incode's QTSP 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.

5.2 Procedural controls

5.2.1 Trusted members

Employees, contractors, consultants can all be considered as trusted people working in a trusted position. Those selected as trusted work in a trusted location that meets CPS requirements.

All employees have the right to access or control encrypted operations that can primarily affect the issuance, use, revocation, cancellation/revocation of digital certificates, including access to to the restricted control area of the CA.

Trustees include all employees, engineers, and consultants whose access to or control of the authentication or encryption process can significantly influence:

- The process of checking information in the Digital Certificate application.
- Acceptance, rejection or other processing of the Digital Certificate application, revocation request, renewal request, or registration information.
- Issue and revoke certificates of employees who have access to restricted parts of the system.

Trusted people include (not limited to):

- Customer service staff.
- System administrator.
- Design Engineer.
- Redundancy engineers and redundancy enforcers manage trust facilities.

5.2.2 Number of people required for each job

Incode has robust security mechanisms and procedures in place to ensure that no single individual can independently perform critical CA operations. This approach enhances security, accountability, and operational integrity through segregation of duties and multi-person control.

1. Multi-Person Control and Segregation of Duties
    - CA operations are never performed by a single individual to prevent unauthorized actions and security risks.
    - This principle ensures shared responsibility, knowledge distribution, and collective control over critical security functions.
2. Role-Based Assignment of Duties
    - Policies and procedures dictate the assignment of duties based on roles and security clearances.

- Highly sensitive tasks, such as accessing and managing cryptographic hardware systems and performing key management operations, require multiple trusted individuals to be involved.

3. Internal Control Procedures for Cryptographic Hardware Access
   - At least three trusted individuals must participate in any physical or logical access to cryptographic hardware that requires strict encryption controls.
   - Sensitive cryptographic operations, such as key generation, signing, and destruction, are conducted under multi-party supervision to prevent security breaches.
   - From initial receipt and verification to the final step of logical or physical destruction, multiple trusted personnel are involved, ensuring compliance, security, and transparency throughout the process.

5.3 Personnel controls

Incode maintains documented policies on personnel control and security for CA and RA systems. Compliance with these policies includes independent audit requirements to ensure adherence to security standards.

These documents contain sensitive and confidential information and are only accessible to parties participating in the QTSP service, subject to Incode's explicit consent.

5.3.1 Competence, experience and other requirements

All Incode employees must receive appropriate training and possess experience in Public Key Infrastructure (PKI) operations, along with the necessary technical and professional competencies.

Additionally, Incode requires employees to have a verified and clear background, ensuring compliance with security and trust requirements.

5.3.2 Background check procedure

Before an employee assumes a trusted role, the QTSP conducts thorough background checks, which include:

- Verification of previous employment history.
- Review of reference information sources.

- Confirmation of relevant professional qualifications and certifications.
- Validation of the candidate's curriculum vitae (CV).
- Assessment of financial and credit history.

As part of the background check process, certain findings may be considered grounds for denying a candidate a trusted position or for taking disciplinary action against existing employees in trusted roles.

5.3.3 Training requirements

Incode organizes necessary training programs to ensure that employees perform their duties professionally and effectively.

Periodic evaluation and reinforcement of these training programs are essential to maintaining competency and compliance.

Training programs are tailored to each employee's specific job responsibilities, ensuring they receive relevant and role-specific knowledge.

5.3.4 Retraining cycle

Incode regularly re-trains and updates its employees with appropriate level and frequency so that employees maintain a level of trust and do their jobs well.

Re-training is required when the system uses new software or features and organizational procedures are implemented.

5.3.5 Discipline for illegal activities

Incode establishes, maintains, and enforces policies against illegal activity. Disciplinary action or termination of contract depending on the seriousness of the illegal action.

5.3.6 Requirements for independent contractors

Independent contractors or consultants can be considered as trustees. Any contractor or consultant is deemed to have the same functions and similar security standards applied to an employee of Incode in a similar position.

5.3.7 Provide documents to employees

Incode provides all the necessary documents for them to do their job well.

5.4 Audit Logging Procedures

5.4.1 Types of Event Logs

The following events are recorded:

- On certificate servers:
  - Start-up and shutdown;
  - Login, logout;
  - Create and sign the certificate.
- On QTSP online servers:
  - Receive a certificate request from an RA;
  - Add a record in the CA's database;
  - Write certificate requests to an external storage device;
  - Transmission of certificates to related party requirements;
  - Store the certificate in an online repository;
  - Received a withdrawal request;
  - Release the CRL.

5.4.2 Event log processing frequency

Audit logs are reviewed to identify relevant and non-recurring alarms within the CA/RA system.

Processing centers compare audit logs with manual or electronic records provided by QTSP customers and Service Centers to investigate any suspicious activity.

Audit Log Processing Includes:

- Reviewing audit logs to identify anomalies and security events.
- Documenting the cause of all significant events in an audit summary.
- Ensuring data integrity by validating that information is not altered or mixed.
- Re-inspecting all recorded data for accuracy and consistency.
- Analyzing alarms or unusual log entries to detect potential security threats.
- Taking appropriate actions based on the findings of the audit log review.

5.4.3 Retention time for record audit

The minimum retention period for audit records is 05 years.

5.4.4 Protection of audit logs

Audit logs will be protected by an electronic audit log system that includes mechanisms to protect the log records from unauthorized access, modification, deletion or tampering. Audit logs are only accessible by the operating system and CA management.

5.4.5 Backup procedure for audit logs

Audit logs will be backed up on a daily basis with changes and additions and weekly full backups.

5.4.6 Accreditation collection system (internal and external)

No specified.

5.4.7 Notice of event cause

No specified.

5.4.8 Weakness Assessment

Not specified.

5.5 Records Archival

5.5.1 Types of records stored

- As described in 5.4.1.
- Information about the electronic certificate application.
- Documentation supporting certificate applications
- Information about the life cycle of electronic certificates, for example, information about certificate revocation and recovery.

5.5.2 Document retention time

Minimum retention period is 5 years.

5.5.3 Secure archives

- Access to archives is strictly limited to authorized executive and administrative staff of Incode.
- All stored data is protected against unauthorized access, viewing, alteration, deletion, modification, or destruction within trusted and secured systems.

- Data storage media and associated applications used to process the data are continuously maintained to ensure that stored information remains accessible and intact for the entire retention period specified in the CPS.

5.5.4 Backup Procedures

- Incode regularly backs up electronic data related to issued certificates to ensure data integrity and security.
- Incremental backups are performed to capture and store changes made to certificate-related data.
- In addition, full backups of all electronic data containing certificate information are conducted weekly to maintain a comprehensive and recoverable record.

5.5.5 Request timestamps for data

All event logs must be timestamped.

5.6 Compromise and Disaster Recovery

5.6.1 Procedures for handling key leaks and incidents

If a subscriber's private key is lost or compromised, the QTSP Registration Authority (RA) must be immediately notified to request the revocation of the affected digital certificate. Additionally, all trusted parties that are aware of and rely on the compromised key should be informed of the situation.

If the QTSP's secret key is compromised, the CA Manager must take the following immediate actions:

1. Notify Subscribers and RAs – Ensure that all affected subscribers and Registration Authorities (RAs) are informed of the compromise.
2. Cease Certificate Issuance and CRL Distribution – Suspend all certificate issuance and stop distributing Certificate Revocation Lists (CRLs) until the issue is resolved.
3. Revoke the Compromised Certificate – Submit a revocation request for the compromised certificate to prevent further usage.
4. Generate a New Key Pair and Certificate – Issue a new QTSP key and certificate, ensuring it is publicly available in the QTSP repository.

5. Revoke All Certificates Signed by the Compromised Key – Invalidate and revoke all active certificates previously issued using the compromised CA key.
6. Publish an Updated CRL – Update and publish a CRL (Certificate Revocation List) reflecting the revoked certificates in the QTSP repository.
7. Notify Security Agencies and Regulatory Authorities – Inform the National Electronic Certification Center and relevant security agencies of the security breach.
8. Notify Trusted Parties and Other CAs – Ensure that all relying parties, trust service providers, and interoperating CAs are aware of the compromise.

5.6.2 Negative behavior towards computer resources, software and data

Incode will make every effort to implement preventive measures and facilitate swift recovery in the event of a system failure. To minimize downtime and resume operations as quickly as possible after a Incode system failure, the following actions will be taken:

- Software Backup – Every software component of Incode is backed up to secure storage media immediately after the installation of a new version of any Incode component.
- CA Data Backup – All active CA data files are backed up on removable storage media after each update or modification.
- If the hardware or software of the signing server fails, the issue will be diagnosed and resolved as quickly as possible.
- If there is uncertainty regarding the extent of unrepaired damage, the server will be completely reinstalled from scratch using original equipment and certified software.
- If data corruption occurs, Incode will diagnose the extent of the damage and restore the affected data from the most recent backup.

5.6.3 The ability to maintain business continuity after a disaster

Incode ensures security measures are in place for the development, testing, and maintenance activities of its Signature. When necessary, Incode will implement a disaster recovery plan, designed to restore critical business functions and information systems efficiently.

- The disaster recovery plan prioritizes the restoration of essential services to ensure minimal disruption.

- The disaster recovery site will have a physical security level defined by Incode to protect infrastructure and data.
- The disaster recovery site is designed to recover or restore data within 24 hours after a disaster occurs.
- The disaster recovery database is regularly synchronized with the production database to ensure data consistency.

5.7 Service Provider Termination

The termination of the service provider requires a formal decommissioning process to ensure the secure transition, revocation, and archival of digital certificates and cryptographic materials, while maintaining regulatory compliance.

In the event that Incode ceases its QTSP services, the following actions will be taken:

1. Notification and Regulatory Compliance
   - Notify the National Regulator to initiate and complete the official termination procedures for service discontinuation.
   - Inform subscribers and RAs as soon as possible, ensuring they have sufficient time to transition to an alternative provider.
   - Issue a large-scale public notice to communicate the termination of operations transparently.
2. Cessation of Certificate Issuance and Continued Support Services
   - Immediately stop issuing new digital certificates upon confirmation of termination.
   - Continue maintaining essential services such as:
     - Issuing CRLs to support relying parties.
     - Maintaining OCSP services for status verification.
   - Revoke all unexpired or previously unrevoked subscriber certificates, if deemed necessary for security or compliance.
3. Financial and Administrative Responsibilities
   - Process refunds for subscribers whose certificates have not yet expired, if required by policy or regulation.
   - Destroy all copies of the QTSP's private key in a secure manner, following cryptographic best practices to prevent unauthorized use.
4. Minimum Notice Period & Record Retention

- A minimum of 60 days' notice will be provided before service suspension in cases of planned termination.
- The CA administrators at the time of termination are responsible for:
  - Retaining all records as required under Section 5.5.2 of the CPS.
  - Executing a structured handover of the CA service to other CAs operating under an existing agreement, if applicable.

6 Technical security control

6.1 Cryptography, private keys and its protections

1. QTSP Key Pair Generation
   - Root CA and Issuer CA keys are generated are generated in a FIPS 140-2 level 3 Hardware Security Module (HSM).
2. Digital Signature Service Provider Key Pair Generation
   - Under the remote digital signing model, the digital signature service provider:
     - Generates the subscriber's key pair, which includes a public and private key, in compliance with Article 3 of Decree 130/2018/ND-CP.
3. Security & Compliance for Key Generation
   - To guarantee that the key pairs are random, unique, and secure, Incode's key generation process:
     - Prevents the private key from being derived from the public key.
     - Follows the PKCS #1 version 2.1 standard for cryptographic key generation.
4. Key Pair Storage and Digital Certificate Issuance
   - The subscriber's key pair is generated on Incode system and securely stored on a HSM.
   - Incode issues digital certificates with a minimum RSA key length of 2048 bits, ensuring strong encryption and preventing the private key from being derived from the public key.

6.2 Computer security control

6.2.1 Specific Computer Security Technical Requirements

Incode ensures that systems containing CA software and data files are secure and resilient against unauthorized access. Additionally, it enforces strict access controls on the main server, limiting access to authorized personnel only. Regular users do not have accounts on the main server.

The computer network is logically segmented into distinct layers, preventing unauthorized access except through predefined processing applications.

All sessions require authentication via passwords or proxy certificates for login.

Direct physical access to the Incode network is restricted to trusted personnel, with access permissions granted based on job roles and responsibilities.

6.2.2 Safety Rating

Incode complies with the ISO 27001 computer system safety standard. Assessment and inspection work is carried out periodically and irregularly based on the actual situation. The system management unit is responsible for handling survey inspection reports and providing measures, plans and implementation to solve the problems in the inspection reports.

6.3 Life Cycle Security Controls

6.3.1 Control on system development

To ensure security, reliability, and compliance, Incode implements the following controls when designing and maintaining software for its CAs and RA:

- Follows a structured Secure Development Lifecycle (SDLC), incorporating security measures at each phase (planning, development, testing, deployment, and maintenance).
- Ensures compliance with industry standards (e.g., eIDAS, ETSI EN 319 411, ISO/IEC 27001, and NIST SP 800-53).
- Implements role-based access control (RBAC) to restrict access to development environments based on job roles.

- Uses multi-factor authentication (MFA) for all developers and administrators accessing the system.
- Conducts regular static and dynamic code analysis to identify vulnerabilities.
- Implements secure coding best practices to mitigate common threats (e.g., SQL injection, buffer overflow, cross-site scripting).
- Maintains code versioning and change tracking through secure repositories.

6.4 Network Security Control

The Certificate Authority (CA) and Registration Authority (RA) functions 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 CA 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.

6.5 Timestamp

Incode operates a Timestamp Authority that complies with RFC 3161

Incode ensures precise clock synchronization, including during leap second events, to maintain the accuracy and reliability of its timestamp server. The server is synchronized at least once every 24 hours with a UTC(k) time source, ensuring compliance with international time standards.

To maintain accuracy, the timestamp server continuously monitors for clock drifts or synchronization anomalies with UTC. If any clock adjustment of one second or greater occurs, it is classified as an auditable event. Similarly, any modifications to the timestamp server's operational processes are also subject to audit.

Furthermore, to uphold cryptographic integrity, the digest algorithm used to sign Timestamp tokens must be identical to the one used for signing the Timestamp certificate. This ensures consistency, security, and trust in the timestamping process.

7 Compliance audits and other assessments

Incode will conduct periodic audits to ensure ongoing compliance with QTSP service standards after its operational deployment. These standards will also serve as a basis for assessments, inspections, and risk management evaluations, ensuring the integrity and security of Incode operations.

Key Compliance and Audit Measures:

- Internal and External Inspections:
    - Incode service standards will be used to evaluate QTSP operations and corporate subscribers.
    - If an audit reveals that Incode fails to meet the required standards, corrective actions will be taken.
    - Depending on the severity and impact of non-compliance, an entity may be allowed to continue operations or may be subject to service suspension or termination.

Risk Management Assessments:

- Incode service standards will be applied to risk assessments conducted by QTSP itself or its subscribers.
    - These assessments will help identify non-compliance issues and outlier results from compliance audits.
    - They will also be integrated into the overall Incode risk management framework.

Audits of Third-Party Entities:

- QTSP service standards will be used to audit, assess, and inspect third-party entities or external audit firms.
- Entities undergoing an audit must fully cooperate with QTSP to ensure a transparent and thorough assessment process.

7.1 Frequency and cases of assessment

- Incode CPS compliance audits will be conducted at least once a year.
- Incode conducts compliance checks of each RA with effective CPS at least once a year.

7.2 Identity and capabilities of the auditor

The audit firm serves as a third-party entity responsible for conducting audits of Incode compliance processes.

The initial assessment and audit will be further reviewed and validated by either:

1. A certified public accounting firm specializing in computer security audits, or
2. Reputable computer security experts appointed by the designated security advisory board.

Additionally, the company must undergo regular audits focusing on IT security and PKI implementation to ensure ongoing compliance with industry standards and regulatory requirements.

7.3 Relationship between auditor and audited entity

Audits conducted by a third-party auditing firm will be performed by entities that are independent of the audited organization. There must be no conflicts of interest that could interfere with the objectivity or integrity of the audit process.

7.4 Subjects in the evaluation process

The areas to be assessed in an assessment required under trust services legislation are those as specified in that legislation, in any other assessment are specified in the technical standards under which the assessment is made.

7.5 Actions Taken as a Result of Deficiency.

Incode must take immediate action if an assessment identifies a violation of the requirements outlined in the Certification Practice Statement (CPS).

If a violation directly impacts the trustworthiness of a certificate, the affected certificate will be revoked immediately to maintain the integrity and security of the Public Key Infrastructure (PKI).

7.6 Result announcement

Assessment result notification is subject to the requirements of trust services legislation and the relevant technical standards.

Assessments results are notified as a written report handed over by the assessor to CEO and the security manager of Incode.

8 Other commercial and legal matters

8.1 Fees

8.1.1 Service fees

The fees of the Service are given by contract concluded between Incode and specific third party (can be flat fee per time period, paying for successful creation of electronic signature etc.).

8.1.2 Fees for other services

Not applicable for the scope of this document.

8.1.3 Fee Refund Policy

Not applicable for the scope of this document.

8.2 Financial responsibility

8.2.1 Insurance coverage

Incode will maintain commercially reasonable coverage for defects or omissions, either through insurance policies with third-party insurers or through self-insurance mechanisms.

However, these claims do not apply to political organizations.

8.2.2 Other properties

Incode has financial autonomy to sustain its operations and fulfill its obligations. Additionally, it is legally responsible for managing risks associated with subscribers and trusted partners.

8.3 Confidentiality of business information

8.3.1 Scope of confidential information

The following subscriber data will be kept confidential and private:

- CA application data, whether approved or unapproved.
- Certificate registration data submitted by the subscriber.
- Enterprise subscriber private keys managed within the PKI, along with the necessary credentials for key recovery.
- Transformation data, including full data records and audit logs related to transformations.
- Audit data collected as part of security and compliance processes.
- Incident and disaster recovery plans, ensuring business continuity and security.
- Security management policies governing the operation of hardware, software, administrators, and certificate services, as well as other critical security services.

Incode ensures that these sensitive data categories remain protected and are only accessed by authorized personnel as required by security policies and regulatory compliance standards.

8.3.2 Information is not within the scope of the confidentiality process

Public information is marked as public.

8.3.3 Responsibility to protect confidential information

Incode ensures the security of private information not to be exposed or disclosed to a third party, except in cases requested by security agencies, state management agencies on authentication services.

8.4 Confidential personal information

8.4.1 Privacy policy

Incode will enforce a strict privacy policy to protect subscriber information. Incode will not disclose the name or any other details related to a subscriber's certificate application to any external party, except when required by competent authorities in accordance with legal or regulatory obligations.

8.4.2 Information that is considered private

All subscriber information that is not publicly available, including issuance certificates, certificate directories and online CRLs is considered private information.

8.4.3 Information is not considered private

Information contained in certificates and CRLs issued by Incode is not considered private. When requesting a certificate from Incode, the subscriber agrees to include this information as part of the published certificate.

8.4.4 Responsibility to protect privacy

Incode is responsible for protecting the privacy of their subscribers and must comply with the privacy laws in their jurisdiction.

8.4.5 Notice and permission to use confidential information

In the event that Incode wish to use private information, permission must be obtained from the owner of such information.

8.4.6 Provide private information as required by law or for administrative processes

Incode is responsible for ensuring the privacy of subscriber information, except in the following cases:

- When required by a competent legal authority or when disclosure is mandated by applicable laws and regulations.
- When information access is requested for administrative purposes, such as verification requests or document creation requests.

8.5 Intellectual property rights

Among the Parties, Incode retains all rights, titles, and interests in its services, software, and technology, including all updates, documentation, products, works, and other intellectual and moral property rights related to them or created, used, or provided by Incode for the purposes of the agreement with the subscriber. This includes copies and derivative works based on the aforementioned assets.

The agreement does not constitute a sale of rights to Incode's services, software, or technology. Instead, it grants the subscriber a right to use these assets under the terms and conditions of the contract. The agreement does not transfer ownership of any

rights in or related to Incode's services, software, or technology, including all updates, documentation, products, works, and intellectual property rights, which remain the exclusive property of Incode.

Additionally, the Incode name and logo, as well as the names of its products associated with its services, software, and technology, are trademarks and/or trade names of Incode. No rights or licenses are granted for their use, unless explicitly specified in the commercial agreement with the subscriber.

8.6 Representations and warranties

8.6.1 CA representations and warranties

Incode does not provide any warranties, guarantees, or assurances regarding its products or services, except as explicitly outlined in this document or in a legally binding agreement with its subscribers. Any descriptions, statements, or implied commitments that are not expressly stated in this document or a formal contract should not be interpreted as representations of Incode's obligations, capabilities, or service guarantees.

Incode's responsibilities and commitments are strictly limited to those set forth in the governing agreements and policies.

8.6.2 Representative of trusted partners and guarantee issues

An agreement with a trusted partner requires the trusted partner to have enough information to make a decision based on the information in the certificate. They are responsible for deciding whether or not to trust the information contained in the deed. Trusted partners will be liable for breach of the trust partner obligations provisions contained in the CPS.

8.6.3 Representation of other stakeholders and guarantee matters

No stipulations.

8.7 Disclaimer of warranties

- The CA does not warrant that its certificate issuance, validation, or revocation services will be uninterrupted, error-free, or continuously available.

- Service availability may be affected by technical failures, scheduled maintenance, or force majeure events.
- The CA makes no warranty that its certificates or services will be fit for any particular purpose beyond those explicitly outlined in this CPS.
- Subscribers and relying parties are responsible for evaluating the suitability of certificates for their intended use.
- All certificates and any related software and services are provided “as is” and “as available”
- To the extent permitted by law, subscription contracts and trust partner contracts may refuse QTSP's guarantee.

8.8 Limitation of Liability

- This document is subject to a system of local and national laws, rules, adjustments, regulations, ordinances and orders, but is not limited or restricted to software exports, hardware and technical information.
- The liability of the parties is regulated and limited according to the signed contract.
- Standalone Provisions: In the event that a provision or amendment of this document is held unenforceable by a trial or other competent hearing, the remainder of the document remains in force

8.9 Indemnities

Customer compensation problem

When required by law, the customer indemnifies QTSP if it appears:

- Invalid information provided by the customer on the certificate issuer.
- Customer error reveals elements related to the application for a certificate, omission due to negligence or with fraudulent purposes.
- Failure of the customer in protecting the secret key, using a trusted system, or not taking the necessary precautions to avoid consequences.
- Use of the customer's name (including without limitation the common name, domain name, or email address) infringes the intellectual property rights of 3rd parties.
- Contracts with customers may contain appropriate additions.

Dealer compensation problem

Where permitted by law, an agreement with the agent shall require the agent to indemnify QTSP :

- An agent's failure to perform a counterparty's duty.
- The agent's confidence in a digital certificate is not met in some cases.
- Agent error in checking the status of the certificate to determine whether the certificate is expired or revoked.
- The agreement with the agent will include a number of additional obligations.

8.10 Term and Termination

8.10.1 Term

This document is effective when published in the archive of the QTSP service. Additional amendments to this document also come into effect upon publication from the archives.

8.10.2 Termination

This document is in effect until it is superseded by a newer version.

8.10.3 The effect of the end and the harm

When the document expires, the components of Incode service will not be limited by the valid terms of the issued certificate.

8.11 Private notice and communication between the parties

Incode will use commercially accepted communication methods to interact with the parties involved. Additionally, if a specific communication method or timeframe is explicitly stated in a signed contract, Incode will follow the terms outlined in that agreement for all relevant communications.

8.12 Amendment

8.12.1 Amendment procedures

Amendments to this document will be made by the appropriate Incode Department. These amendments may be issued as either:

1. A separate document detailing all amendments to the document, or
2. An updated version of the document incorporating the changes.

The revised or updated version will be linked in the Notifications and Updates section of the QTSP service archive, available at https://psc.incode.com/qtsp-legal-repository/

8.12.2 Cases where object identification (OID) modification is required

No OID is assigned to this Policy, it covers OIDs as defined in chapter 1.2. Any change to this Policy results in a new version of the document.

8.13 Dispute resolution

To the extent permitted by applicable law, all Subscriber Agreements and Relying Party Agreements shall include a dispute resolution clause.

Unless otherwise approved by Incode, disputes involving Incode must follow a structured resolution process, which consists of:

1. An initial negotiation period of sixty (60) days to attempt an amicable resolution.
2. If no resolution is reached, the dispute may proceed to litigation in a court with the appropriate jurisdiction.

Disputes Related to the CPS

- Disputes arising from the Certification Practice Statement (CPS) will be handled by QTSP's CPS Manager.

Contractual Disputes

- Disputes between QTSP, collaborators, and subscribers must be resolved according to the terms of the respective contract.
- Disputes between QTSP and its agents must be settled according to the terms of the Affiliate Contract.
- If no resolution is achieved within the 60-day negotiation period, the matter may be escalated to court with the appropriate jurisdiction.

8.14 Council Law

The operation of Incode must comply with the laws of the Czech Republic, including:

- The relevant national legislation governing Incode operations
- The Czech Republic's e-commerce laws

All disputes arising from:

- The terms and provisions of this CPS
- The activities of the CA and RA
- The use of QTSP services
- The issuance, acceptance, or use of any certificate issued by Incode

Shall be resolved in accordance with the applicable laws of the Czech Republic and through the dispute resolution procedures outlined in the relevant agreements.

8.15 Compliance With Applicable Law

All activities related to this CPS must comply with the laws of the of Czech Republic.

8.16 Mixed Terms

Do not apply.

8.17 Other provisions

Do not apply.