incode psc

Certificate Policy Statement

Version	Modified by	Modifications made	Date modified
1.0	LV	Content	12/2024
1.1	LV	OID adjustment, inclusion of additional email addresses for contact, and refinements to Section 4.10.1.7.	03/2025

Tabla de contenido

1 INTRODUCTION 8

1.1 Overview 8
1.2 Document name and identification 9
1.3 PKI Participants 9
1.3.1 Incode Root Certificate Authority 9
1.3.2 Incode Intermediate or Issuing CA 9
1.3.3 Registration Authority (RA) 10
1.3.4 Subscribers 10
1.3.5 Relying parties 12
1.3.6 Other participants 12
1.4 Certificate Usage 13
1.4.1 Appropiate certificate usage 13
1.4.2 Prohibited Certificate Uses 13
1.5 Policy management 15
1.5.1 Incode Department Responsible for the Policy 15
1.5.2 Contact Person 15
1.5.3 Revocation Contact 15
1.6 Definitions and Abbreviations 16
1.6.1 Definitions 16
1.6.2 Acronyms 18

2 RESPONSIBILITY FOR PUBLICATION AND STORAGE 19

2.1 Storage 19
2.2 Disclosure of certificate information 21
2.3 Information disclosure frequency 21
2.4 Control access to the repository 21

3 IDENTIFICATION AND AUTHENTICATION 22

3.1 Name convention 22
3.2 Types of Names 22
3.3 Need for Names to be Meaningful 23
3.4 Anonymity or Pseudonymity of Subscribers 23
3.5 Rules for Interpreting Various Name Forms 24
3.6 Uniqueness of Names 24
3.7 Recognition, Authentication, and Role of Trademarks 24
3.7.1 Issuer CA Rights in Case of Disputes 24
3.8 Initial identity verification 25
3.8.1 How to prove possession of secret key 25
3.8.2 Identification and authentication for individual subjects 25
3.9 Services for people with disabilities 26
3.10 Identification and authentication for re-key requests 27
3.10.1 Identification and authentication for routine re-key 27
3.10.2 Identify and authentication for re-key after revocation 27
3.11 Identification and authentication for revocation request 28

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 29

4.1 Certificate Application 29
4.1.1 Who can submit a certificate application? 29
4.2 Enrollment 29

4.3 Certificate Application Processing 30
4.3.1 Identification and Authentication Process 30
4.3.2 Accept or refuse to issue digital certificates 30
4.3.3 Processing time for a certificate request 31
4.4 Issuance of certificates 31
4.4.1 Actions performed by the CA during the issuance of the certificate 31
4.4.2 Notifications to the subscriber or applicant of the certificate 32
4.5 Acceptance of the certificate 33
4.5.1 Conducts constituting certificate acceptance 33
4.5.2 Publication of QTSP 's certificate 33
4.6 Key Pair and Certificate Usage 34
4.6.1 Using the subscriber's certificate and private key 34
4.6.2 Relying party public key and certificate usage 35
4.7 Certificate Renewal 36
4.7.1 Renewal Eligibility and Conditions 37
4.7.2 Processing requests for renewal of digital certificates 37
4.7.3 Notice to subscribers about the issuance of new digital certificates 37
4.7.4 Terms of accepting renewal of digital certificates 37
4.7.5 Announcement of extended digital certificates 37
4.8 Certificate Re-Key 38
4.8.1 Who may request certificate re-key? 38
4.8.2 Processing new key requests for certificates 38
4.8.3 Notice of release of new certificates to subscribers 38
4.8.4 Notice of acceptance of new issuance of certificate keys 38
4.8.5 Issuing a certificate that has been issued with a new key of QTSP 38
4.8.6 Notice of issuance of certificates of QTSP to other entities 38
4.9 Certificate modification 38
4.9.1 Cases of modifying certificates 38
4.9.2 Subject of request for certificate modification 39
4.9.3 Certificate modification request processing 39
4.9.4 Notice of release of new certificates to subscribers 39
4.9.5 Conditions for accepting subscription modifications 39
4.9.6 Issuance of modified certificates from QTSP 39
4.9.7 Notice of issuance of certificates of QTSP to other entities 39
4.10 Certificate Revocation and Suspension 39
4.10.1 Certificate Revocation 39
4.10.2 Certificate Suspension 43
4.11 Certificate Status Service 43
4.11.1 Operational characteristics 43
4.11.2 Service availability 43
4.11.3 Optional features 44
4.12 End of subscription 44
4.13 Key scrow and recovery 44

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS 44

5.1 Physical level control 44
5.1.1 Physical access 45
5.1.2 Air condition and power supply 45
5.1.3 Contact with water 45
5.1.4 Fire protection and prevention 46
5.1.5 Storage media 46
5.1.6 Garbage treatment and destruction 46

5.1.7 *Remote backup* 46
5.2 PROCEDURAL CONTROLS 46
5.2.1 *Trusted members* 46
5.2.2 *Number of people required for each job* 47
5.3 PERSONNEL CONTROLS 48
5.3.1 *Competence, experience and other requirements* 48
5.3.2 *Background check procedure* 49
5.3.3 *Training requirements* 49
5.3.4 *Retraining cycle* 49
5.3.5 *Discipline for illegal activities* 50
5.3.6 *Requirements for independent contractors* 50
5.3.7 *Provide documents to employees* 50
5.4 AUDIT LOGGING PROCEDURES 50
5.4.1 *Types of Event Logs* 50
5.4.2 *Event log processing frequency* 50
5.4.3 *Retention time for record audit* 51
5.4.4 *Protection of audit logs* 51
5.4.5 *Backup procedure for audit logs* 51
5.4.6 *Accreditation collection system (internal and external)* 51
5.4.7 *Notice of event cause* 51
5.4.8 *Weakness Assessment* 52
5.5 RECORDS ARCHIVAL 52
5.5.1 *Types of records stored* 52
5.5.2 *Document retention time* 52
5.5.3 *Secure archives* 52
5.5.4 *Backup Procedures* 52
5.5.5 *Request timestamps for data* 53
5.6 KEY CHANGEOVER 53
5.7 COMPROMISE AND DISASTER RECOVERY 53
5.7.1 *Procedures for handling key leaks and incidents* 53
5.7.2 *Negative behavior towards computer resources, software and data* 54
5.7.3 *The ability to maintain business continuity after a disaster* 55
5.8 CA OR RA TERMINATION 55

6 TECHNICAL SECURITY CONTROL 57

6.1 GENERATE KEY PAIR AND SETTINGS 57
6.1.1 *Generate key pair* 57
6.1.2 *Transfer the secret key to the subscriber* 58
6.1.3 *Transfer the public key to the certificate authority* 58
6.1.4 *Transfer CA's public key to trusted partners* 58
6.1.5 *Key size* 58
6.1.6 *Generate parameters for the public key and check the quality* 59
6.1.7 *Key use purpose (as in X.509 v3 key usage field)* 59
6.2 PROTECT THE SECRET KEY AND CONTROL THE ENCRYPTION METHOD 60
6.2.1 *Cryptographic module standards* 60
6.2.2 *Multiple secret key control* 60
6.2.3 *Private key scrow* 61
6.2.4 *Private key backup* 61
6.2.5 *Private key archival* 61
6.2.6 *Private key storage on cryptographic modules* 62
6.2.7 *Private key activation* 62
6.2.8 *Private key deactivation* 62

6.2.9 Private key destruction *62*
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 62
6.3.1 Public key archival *62*
6.3.2 Certificate Operational Periods and Key Pair Usage Periods *63*
6.4 COMPUTER SECURITY CONTROL 63
6.4.1 Specific Computer Security Technical Requirements *63*
6.4.2 Safety Rating *63*
6.5 LIFE CYCLE SECURITY CONTROLS 64
6.5.1 Control on system development *64*
6.5.2 Security Management Control *64*
6.5.3 Security control over a lifecycle *64*
6.6 NETWORK SECURITY CONTROL 64
6.7 TIMESTAMP 65

7 FORMAT OF CERTIFICATES, CRL AND OCSP 66

7.1 CERTIFICATE PROFILE 66
7.1.1 Version *66*
7.1.2 Certificate extension *66*
7.1.3 Algorithm number *68*
7.1.4 Name Form *69*
7.1.5 Name constraints *69*
7.1.6 Certificate Policy OID *70*
7.1.7 Usage of binding policy extension *70*
7.1.8 Semantic handling for the extension of important certificates *70*
7.2 CRL PROFILE 70
7.2.1 Version *70*
7.2.2 CRL and CRL entry extensions *70*
7.3 PROFILE OF OCSP 72
7.3.1 Version *72*
7.3.2 OCSP Extensions *72*

8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS 72

8.1 FREQUENCY AND CASES OF ASSESSMENT 73
8.2 IDENTITY AND CAPABILITIES OF THE AUDITOR 73
8.3 RELATIONSHIP BETWEEN AUDITOR AND AUDITED ENTITY 74
8.4 SUBJECTS IN THE EVALUATION PROCESS 74
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY. 75
8.6 RESULT ANNOUNCEMENT 75

9 OTHER COMMERCIAL AND LEGAL MATTERS 75

9.1 FEES 75
9.1.1 Fee for issuance of Certificate or renewal of certificate *75*
9.1.2 Fees for using certificates *75*
9.1.3 Fees for accessing information about certificate status and certificate revocation *75*
9.1.4 Usage fees for other services *76*
9.1.5 Fee Refund Policy *76*
9.2 FINANCIAL RESPONSIBILITY 76
9.2.1 Insurance coverage *76*
9.2.2 Cases where QTSP conducts insurance compensation *77*
9.2.3 Cases that are not covered by insurance *77*
9.2.4 Other properties *77*
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 78

9.3.1 Scope of confidential information 78
9.3.2 Information is not within the scope of the confidentiality process 78
9.3.3 Responsibility to protect confidential information 78
9.4 CONFIDENTIAL PERSONAL INFORMATION 79
9.4.1 Privacy policy 79
9.4.2 Information that is considered private 79
9.4.3 Information is not considered private 79
9.4.4 Responsibility to protect privacy 79
9.4.5 Notice and permission to use confidential information 79
9.4.6 Provide private information as required by law or for administrative processes 79
9.5 INTELLECTUAL PROPERTY RIGHTS 80
9.6 REPRESENTATIONS AND WARRANTIES 80
9.6.1 CA representations and warranties 80
9.6.2 RA representation and warranties 81
9.6.3 Suscriber representation and warranties 82
9.6.4 Representative of trusted partners and guarantee issues 83
9.6.5 Representation of other stakeholders and guarantee matters 83
9.7 DISCLAIMER OF WARRANTIES 83
9.8 LIMITATION OF LIABILITY 84
9.9 INDEMNITIES 84
9.10 TERM AND TERMINATION 85
9.10.1 Term 85
9.10.2 Termination 85
9.10.3 The effect of the end and the harm 85
9.11 PRIVATE NOTICE AND COMMUNICATION BETWEEN THE PARTIES 85
9.12 AMENDMENT 85
9.12.1 Amendment procedures 85
9.12.2 Cases where object identification (OID) modification is required 86
9.12.3 How and when to notify 86
9.13 DISPUTE RESOLUTION 86
9.14 COUNCIL LAW 87
9.15 COMPLIANCE WITH APPLICABLE LAW 88
9.16 MIXED TERMS 88
9.17 OTHER PROVISIONS 88

1 Introduction

1.1 Overview

This document serves as the Certificate Policy Statement (CPS), which defines the governance policies of Incode as a Qualified Trust Service Provider (QTSP) in the provision of digital signature services. It outlines the certification framework for remote digital signatures, specifying how digital certificates are issued, managed, used, revoked, and reissued..

The CPS requirements, designed to ensure the security and integrity of the QTSP service, apply to all participants in Incode's digital signature certification ecosystem. This document is structured in accordance with RFC 3647 (IETF Certificate Policy and Certification Practice Statement).

The CPS serves as a statement of obligations undertaken by the QTSP for customers using its digital signature certification service. It is important to note that the CPS does not constitute a legal agreement between the QTSP 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 electronic certificates and does not extend to other services provided by the QTSP.

1.2 Document name and identification

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

The OID for this Certification Policy is **1.3.6.1.4.1.22635891.1.1.1**, 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].[codeCA].[codeCAPS]

Where:

- TypeCA identifier = 1 (public).
- QTSP codeCA identifier = 2.
- codeCAPS identifier = 1.

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

Document name: QTSP Authentication Regulations according to the remote digital signing model.

1.3 PKI Participants

1.3.1 Incode Root Certificate Authority

Incode Root Certificate Authority (Root CA) is the highest-level entity in Incode's PKI that is responsible for issuing and managing digital certificates. It acts as the trust anchor for the entire PKI ecosystem, ensuring the authenticity, integrity, and security of all certificates issued under it.

- Incode Root CA does not typically issue certificates directly to end-users.
- Signs and issues certificates for Intermediate (Subordinate) CAs, which then issue certificates to end-entities (e.g., individuals, organizations, or devices)

1.3.2 Incode Intermediate or Issuing CA

Incode Intermediate Certificate Authority (Intermediate CA), also known as a Subordinate CA, serves as a bridge between it's Root CA and end-entity certificates in it's PKI.

In Incode architecture, Issuing CA is a specific type of Intermediate CA that is directly responsible for issuing end-entity certificates, such as TLS/SSL certificates, digital signatures, or authentication certificates.

1.3.3 Registration Authority (RA)

Registration Authorities (RAs) serve as the authenticating entities responsible for verifying certificate requests from customers. The Qualified Trust Service Provider (QTSP) and its designated affiliates acting as RAs oversee the issuance and lifecycle management of digital certificates, ensuring compliance with regulatory and security standards.

Additionally, QTSP affiliates may establish contractual agreements with businesses that wish to manage their own certificate issuance. In such cases, these corporate clients may function as their own RAs, validating credential requests for:

- Themselves, for internal corporate use.
- Individuals or organizations within their hierarchy, such as employees, partners, or subsidiaries.

To maintain impartiality and compliance, the Registry Officer—responsible for approving service operation—must operate without conflicts of interest. The officer cannot be involved in both the request initiation and approval processes to ensure the integrity, neutrality, and security of the certificate issuance workflow.

The QTSP or its designated affiliate retains overall accountability for adherence to certification standards and assumes full responsibility for the validity and security of all issued certificates..

1.3.4 Subscribers

Subscribers of the Qualified Trust Services of Incode could be natural or legal persons or system that is issued a digital certificate by Incode. Subscribers use these certificates to perform secure communications, authentication, encryption, and digital signing within the PKI framework. A Subscriber is not required to be the Subject of certificates under its control.

1.3.4.1 Subscriber's rights:

- Subscribers are granted a digital certificate based on the type of certificate requested.
- The subscriber's digital certificate remains valid and active throughout its designated validity period.
- Subscribers are authorized to use digital signature services and authenticate digital signatures under the remote digital signature model, in accordance with the validity period specified in the service contract.
- Subscribers have the right to request renewal or revocation of their digital certificates.
- Subscribers have the right to confirm all actions related to their private key through their registered device.
- Subscribers have the right to renew, suspend, or cancel the digital signature service and authenticate digital signatures under the remote digital signature model.

1.3.4.2 Obligations of Subscriber:

- All commitments made by subscribers in their digital certificate application are accurate and truthful.
- All information provided by the subscriber and included in the digital certificate is correct and up to date.
- Digital certificates must only be used for lawful purposes and must comply with the Certification Practice Statement (CPS) and regulations set by relevant authorities.
- Subscribers must not forge or tamper with QTSP's digital certificates.
- Any changes in subscriber information must be immediately reported to the designated QTSP service entry point.
- Subscribers must request revocation of digital certificates in cases of errors or security issues that may impact the integrity of QTSP's digital certificates.

1.3.5 Relying parties

The relying party is the entity that trusts the digital certificate or digital signature issued by the QTSP. Depending on the regulations governing the use of digital certificates, the recipient may or may not be a subscriber of the QTSP. The relying party:

- Bases trust on the digital certificate provided by the QTSP.
- Decides whether to accept or reject the certificate when verifying electronic transactions.
- Must adhere to the terms outlined in the Relying Party Agreement (RPA) associated with the certificate.

1.3.5.1 Recipient's rights:

- The relying party has the right to verify the accuracy of the subscriber's information contained in the digital certificate.
- The relying party makes decisions regarding agreements and commitments based on the verified information in the digital certificate and the details outlined in the Certification Practice Statement (CPS).

1.3.5.2 Obligations of the receiver

- Receive notices from QTSP about cooperation conditions for 3rd parties.
- Only trust the digital certificate provided by QTSP if it is valid when checked and updated regularly.
- Only trust a digital certificate if it has not been revoked.
- Only trust the QTSP mobile application provided by QTSP, which is announced on the official website of the QTSP service
- Immediately notify CA/RA if it is suspected that the secret key has been exposed, stolen, modified or destroyed;
- CA/RA must be notified immediately if it is suspected that the QTSP application on the phone shows signs of being corrupted, copied or the PIN code is exposed.

1.3.6 Other participants

No stipulation.

1.4 Certificate Usage

Subscribers and Relying Parties must strictly adhere to the applicable agreements when using digital certificates. Given the varying sensitivity of the information protected by publicly trusted certificates, each Relying Party bears full responsibility for assessing potential risks and verifying the certificate's validity before placing trust in it.

1.4.1 Appropiate certificate usage

Digital certificates issued in accordance with this CPS may be used for the purposes designated in the key usage and extended key usage fields defined in the certificate. However, the sensitivity of the information that will be processed or protected by a digital certificate depends on the environment in which it is applied. Each relying party must assess the application environment and associated risks before deciding whether to use a digital certificate issued in accordance with this CPS.

Certificates are issued for different security functions, and their usage is typically classified as follows:

- **Authentication** – Used to verify the identity of a user, device, or system.
- **Digital Signatures** – Provides integrity and non-repudiation for signed documents and transactions.
- **Encryption** – Secures communications by encrypting data.
- **Code Signing** – Ensures the authenticity and integrity of software applications.
- **Time Stamping** – Verifies the existence of data at a particular time.

The certificates must be used in accordance with the provisions of the law in UE.

1.4.2 Prohibited Certificate Uses

Incode strictly prohibits taking advantage of the use of digital signatures to oppose the State, disrupt security, order and safety, carry out smuggling activities or conduct other activities contrary to the law, societal morality.

Digital certificates issued in accordance with this CPS may not be used in the following scenarios:

1. As a Subordinate Entity of Incode's Certification Authority

a. Certificates issued under this policy must not:
b. Be used to sign other certificates.
c. Act as certification agents.
d. Function as a Certification Authority (CA).
e. Sign Certificate Revocation Lists (CRLs).
f. Sign services issued under the OCSP (Online Certificate Status Protocol).

2. In Applications Requiring Fail-Safe Performance

Certificates must not be used in systems where failure could result in serious harm, including:

a. Operation of electrical power facilities.
b. Traffic control systems (land, air, etc.).
c. Aircraft navigation systems.
d. Any other system where a failure could lead to injury, loss of life, or environmental damage.

3. Where Prohibited by Law

Certificates must not be used in any scenario where their usage is expressly prohibited by applicable laws or regulations.

Additionally, certificates must be used only for their designated purposes. Common restrictions include:

- TLS certificates must not be used for document signing.
- Code signing certificates must not be used for email encryption.
- End-entity certificates must not be used to issue other certificates (reserved for CA certificates only).

This ensures compliance with security policies and prevents improper or unauthorized use of certificates.

1.5 Policy management

1.5.1 Incode Department Responsible for the Policy

The CPS, along with documents related to the operation of Incode as QTSP and its Registration Authorities (RAs), are managed, supported, and supervised by Incode's Security and Compliance Department, which is responsible for its maintenance and updates.

A review of the procedures established in this CPS 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 Security and Compliance Department is responsible for determining the applicability of the CPS and its associated policies.

1.5.2 Contact Person

- Incode Czech Republic, LLC
- PSC Operation Manager
- Pujmanové 1753/10a, Nusle, 140 00 Prague 4
- psc@incode.com

1.5.3 Revocation Contact

- Incode Czech Republic, LLC
- Revocation Agent
- Pujmanové 1753/10a, Nusle, 140 00 Prague 4
- revocations@incode.com

Incode will approve the CPS. Each instance of CPS has a unique object identifier (OID). CPS changes, updates are recorded in a document containing CPS amendments or information about the update process and are published at https://psc.incode.com/qtsp-legal-repository/

1.6 Definitions and Abbreviations

1.6.1 Definitions

Terms	Explain
Certificate No. QTSP	Is a form of electronic certificate issued by QTSP.
Valid digital certificate	Is a digital certificate that has not expired, is not suspended or revoked.
Digital signatures	A form of electronic signature created by transforming a data message using an asymmetric cryptographic system whereby the person possessing the original data message and the signer's public key can determine be exact: - The above transformation is generated with the correct private key corresponding to the public key in the same key pair; - Content integrity of the data message since the above transformation is performed.
Digital signature authentication service	Is a type of electronic signature authentication service, granted by a digital signature certification service provider. Digital signature certification services include: - Generate key pair including public key and private key for subscriber; - Issue, renew, suspend, restore and revoke digital certificates of subscribers; - Maintain online database of digital certificates; - - Other related services as prescribed.
Asymmetric cryptosystem	A cryptographic system capable of generating a key pair consisting of a private key and a public key.
Lock	A sequence of binary numbers (0 and 1) used in cryptographic systems.
Secret key	A key in a key pair of an asymmetric cryptosystem used to create digital signatures.

Terms	Explain
Public key	A key in a key pair of an asymmetric cryptosystem, used to verify the digital signature generated by the corresponding secret key in the key pair.
Digital signature	The introduction of a secret key into a software program that automatically generates and affixes a digital signature to a data message.
Signer	A subscriber who uses his/her own private key to digitally sign a data message under his/her name.
Receiver	An organization or individual that receives a data message digitally signed by a signer, uses that signer's digital certificate to check the digital signature in the received data message and conducts activities and transactions. related.
Subscribers	An organization or individual that is granted a digital certificate, accepts a digital certificate and keeps a secret key corresponding to the public key recorded on that issued digital certificate.
Suspend digital certificate	Is to invalidate a digital certificate temporarily from a specified time.
Revocation of digital certificate	Is to invalidate a digital certificate permanently from a specified time.

1.6.2 Acronyms

Symbol	Full name
SHIFT	Certificate Authority / Certification Authority
AC	Access Control – Manage access
Administrator	Super admin rights for Signer SAM
AES	Advanced Encryption Standard - Advanced encryption standard
APNs	Apple push notification service – Apple's messaging service
CC	Common Criteria
CGA	Certificate Generation Application – a service that allows signers to issue digital certificates
CM	Cryptographic Module – embedded in HSM . device
CMS	Cryptographic Message Syntax
CP	Certificate Policy / Certificate Policy
CPS	Certification Practice Statement / Certification Policy
CRLs	Certificate Revocation Lists / DS certificate of revocation
CSP	Certificate Service Provider – a service that allows the end user to be associated with a public key and a signer identifier
CSR	Certificate Signing Request – request to issue a digital certificate
DES	Data Encryption Standard / Data Encryption Standard
DNS	Domain Name System
DTBS	Data To Be Signed – signed data/documents
DTBS/CHEAP	Data To Be Signed Representation – DTBS/R is generated from DTBS with hash algorithm
EAL	Evaluation Assurance Level
FCM	Firebase Cloud Messaging

Symbol	Full name
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module – hardware that digitally signs and stores the secret key
HSM Master Key	Hardware Security Module master key - HSM's master key is used to encrypt other keys for data encryption that the system wants to protect. This master key can decrypt other keys and also decrypt the data indirectly
HTTPS	Secure Hypertext Transaction Standard
ICT	Information and Communications Technology
iDP	Identity Provider – Authentication Service Provider
keyUUID	Key Universally Unique IDentifier – D.Signing_Key_ID is referenced as key UUID with unique identifier for end user signing key
KTK	Key Transfer Key – the key used to encrypt other keys for transfer in transit from components of the RSSP system

2 Responsibility for publication and storage

2.1 Storage

Incode is responsible for maintaining the online issuance and management of digital certificates. Certificate storage ensuring that users can access QTSP-issued digital certificates and CRLs when needed. Additionally, service-related documents, including the CPS, are available through the Incode web page or through the Contact Person defined in Policy Management section.

1. Continuous Availability and System Infrastructure

Incode ensures 24/7 availability of valid and expired digital certificates by managing dedicated functional servers that support:

- Certificate Revocation Lists (CRL)
- Online Certificate Status Protocol (OCSP) responses

These servers are:

- Located in a public network partition with high-speed broadband connectivity.
- Hosted within QTSP's Data Center, which features:
  - A stable internet connection
  - High-speed infrastructure
  - Controlled environmental conditions
  - A stable power supply
  - A dedicated technical team maintaining 24/7 service continuity and system availability

2. Certificate Revocation Lists (CRLs) and Relying Party Responsibilities

The CRL is a list of serial numbers corresponding to revoked digital certificates, published by the QTSP service provider. Relying parties involved in transactions must:

- Check the CRL to verify certificate validity.
- Reject any certificates listed in the CRL.

A CRL is stored in the service provider's public directory and is generated:

- Periodically, within a defined time frame.
- Immediately after a certificate is revoked or suspended.

Incode system automatically and periodically updates information on valid and expired digital certificates. The CRL is stored on a dedicated CRL repository, ensuring 24/7 online access via protocols such as HTTP/HTTPS.

3. Retention of Revocation and Subscriber Data

All information related to certificate revocation, subscriber databases, and digital certificates must be retained for a minimum of five (5) years from the date the certificate is suspended or revoked.

2.2 Disclosure of certificate information

Public digital signature certification organization according to the remote digital signature model QTSP performs secure online storage of information including:

- Digital certificate of QTSP;
- CRLs;
- Online Certificate Status Service (OCSP);
- Digital certificate issued by QTSP ;
- QTSP's Certificates and CPS and earlier versions;
- Other relevant information.

2.3 Information disclosure frequency

The QTSP digital certificate will be published immediately upon the subscriber's acceptance, in accordance with the procedures required by the QTSP.

The CRL is updated at least every 24 hours and is automatically generated by the QTSP system.

CPS Publication Frequency: A new version of the CPS will be published immediately upon approval, while the previous version will be securely archived.

The system automatically and continuously updates the list of valid and expired digital certificates within the database and directory system.

Certificate validity can be verified online 24/7 via the OCSP and CRL services, ensuring continuous and reliable access.

2.4 Control access to the repository

Incode does not require authentication for third-party access to the CRL, QTSP digital certificates, and CPS through the designated online disclosure address.

Any modifications to the CPS or digital certificates of QTSP service providers may only be made by authorized Incode authorities.

3 Identification and Authentication

3.1 Name convention

Incode's Certification Authority (CA) follows the references and standards outlined in RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" for the encoding of the certificates it issues.

The "Subject" field of a digital certificate complies with the X.509 v3 standard. The content of the "Subject" field includes, at a minimum and depending on the certificate profile, the following components:

- Common Name (CN): A unique identifier for each organization, individual, host, or service.
- UUID: A unique identifier, predefined according to QTSP's administrative rules.
- Organization (O): The official name of the organization, predefined based on QTSP's administrative rules.
- Organizational Unit (OU): The specific department or division within the organization.
- Locality Name (L): A predefined location name, based on QTSP's administrative rules.
- State Name (S): The predefined state or province name, according to QTSP's administrative rules.
- Country Name (C): ISO 3166 country code.

Special Requirements Based on Certificate Type

- For digital certificates issued to individuals:
  - The "Subject" field must include the subscriber's first and last name.
- For digital certificates issued to hosts/servers:
  - The "Subject" field must include the Fully Qualified Domain Name (FQDN) of the host/server.

3.2 Types of Names

As part of the digital certificate issuance process, Incode must ensure that the "Distinguished Name" (DN) field is not null or empty, in compliance with the ITU X.500 standard.

Each digital certificate issued by Incode's CA contains:

- The Distinguished Name (DN) of the issuing CA.
- The Distinguished Name (DN) of the certificate holder.

This field serves to identify key information about both entities and acts as a reference in processes where the issued certificate is utilized.

The DN attributes may vary depending on the certificate profile used during issuance. However, all profiles must at a minimum include:

- The Common Name (CN).
- The country where the certificate issuance request was made.

3.3 Need for Names to be Meaningful

As part of this CPS, Incode establishes that the Common Name attribute of the certificate holder must be representative. This means it must allow relying parties to clearly identify the certificate holder in transactions where the certificate is used for authentication.

For this purpose:

- For individual (natural person) certificates, only the legal name as stated in the identity documents presented during the identity verification process will be accepted.
- Special characters will not be permitted as part of the name in certificates.
- For individuals representing an organization, the business may include the position and role of that organization. In case the subscriber is an organization, the business will reflect the registered name under the law of that subscriber.
- Where a digital certificate points to a role or location, it must also include the identity of the person holding that role or position.
- A digital certificate issued to an electronic device must include either the authenticated name of the electronic device or the name of the person or entity responsible.

3.4 Anonymity or Pseudonymity of Subscribers

Incode aims to ensure that the digital certificates it issues enable the identification of individuals and organizations in electronic transactions and processes. Therefore, the **use of pseudonyms** when requesting a certificate **is not permitted**.

Additionally, anonymous certificate requests will be automatically rejected by Incode's CA, as they do not comply with the requirements outlined in the previous section of this CPS.

3.5 Rules for Interpreting Various Name Forms

The digital certificates issued by Incode's Certification Authority (CA) are generated in compliance with the international standard RFC 3280, *"Internet X.509 Public Key Infrastructure."* This standard defines the structure and technical specifications that certificates must adhere to.

These specifications establish the rules for identifying and interpreting the Distinguished Names (DNs) of both certificate holders and the Certification Authority (CA) itself.

In accordance with this standard, certificates issued by Incode's CA use UTF8String encoding.

3.6 Uniqueness of Names

The subject name stated in the digital certificate must be clear and unique to all digital certificates issued by the Issuer CA, and conform to the X.500 standard for name uniqueness. When necessary, numbers or characters can be added to the original name to ensure the uniqueness of the name in the entire catalog of digital certificates issued by the CA. Any arbitrary naming is not allowed here. Each name will have to be unique to the unique subscriber.

3.7 Recognition, Authentication, and Role of Trademarks

Need for Names to be Meaningful Section of this CPS defines the naming requirements for individuals and legal entities requesting a digital certificate from Issuer CA.

As a result, any certificate application submitted with a name that differs from the legally recognized name of an individual or legal entity, as stated in their official supporting documents, will be rejected.

Additionally, as part of its procedures, Issuer CAs does not verify the ownership of trade names or registered trademarks, nor does it include them in digital certificates, as their use is explicitly restricted under this policy.

3.7.1 Issuer CA Rights in Case of Disputes

Issuer CAs have the right to reject or revoke any certificate application in the event of a naming dispute, without incurring any liability to the applicant.

3.8 Initial identity verification

3.8.1 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.

3.8.2 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 & Usage

- If the verification is successful and a One-Time or Short-Term certificate is required, it is issued with specific:
  - Limited validity (e.g., minutes to a few days).
  - Restricted usage scope (e.g., a single transaction, single session, document signing, authentication).
- If the verification is successful and a Long-Term certificate is required:
  - Certificate is issued with long time validation (e.g. months to years)
  - The certificate is delivered to the applicant via:
    - Secure download
    - Mobile or web-based storage
    - Integration into a cryptographic module or key store

6. 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.

3.9 Services for people with disabilities

- Incode provides services for people with disabilities in accordance with current laws in Czech Republic.
- Incode strives to ensure equal access to the services provided by the company to the highest possible standards. To establish equal opportunities for services, Incode takes all possible and reasonable steps to provide its services without impeding persons with disabilities. It is especially important to ensure that clients with disabilities receive services

tailored to their special needs, of the same quality as services for other customers. .

- Incode works with clients to secure them an administrative regulation that best suits their individual needs within the framework defined by CPS.

3.10 Identification and authentication for re-key requests

3.10.1 Identification and authentication for routine re-key

During the validity period of QTSP's digital certificates, Incode subscribers may request the issuance of a new digital certificate with a new key pair.

Key re-issuance before the certificate's expiration is performed by submitting a key reissue request, which includes the new public key and is digitally signed with the old private key, to the QTSP Registration Authority (RA). The RA ensures that the individual or organization requesting the key re-issuance is the rightful subscriber of the original digital certificate.

To approve a subscriber's re-key request, the RA must verify that the subscriber's identity and information remain unchanged and accurate. After key re-issuance, the QTSP CA or RA will reconfirm and authenticate the subscriber following the same verification requirements as the original certificate application.

If the subscriber loses the private key, they must request certificate revocation and follow the appropriate process as described in the following section.

3.10.2 Identify and authentication for re-key after revocation

Digital certificates that have been revoked or expired are permanently invalid and cannot be re-keyed, renewed, or updated under any circumstances. Any new certificate request following revocation or expiration must undergo the full initial registration process without exception.

3.11 Identification and authentication for revocation request

Subscribers may request the revocation of their digital certificates at any time and for any reason. However, to prevent unauthorized revocation requests, Incode implements an authentication mechanism to verify the legitimacy of such requests, particularly when they are submitted electronically.

- When a revocation request is sent electronically, the subscriber's identity must be authenticated using a digital signature.
- If the request is signed with the private key corresponding to the public key of the requester, it will be accepted and considered valid.

Submission and Processing of Revocation Requests

- All digital certificate revocation requests must be submitted to the QTSP or its Registration Authority (RA), either:
  - Through an approved online process, or
  - In writing, following the prescribed revocation procedure.
- The CA will record and retain all authenticated revocation requests and any corresponding actions in compliance with regulatory requirements.
- If a digital certificate is revoked, an evaluation report of the revocation will be stored in the system for audit and security purposes.
- Once revoked, the certificate's status will be updated and published in the CRL and OCSP service of Incode.

Emergency Revocation in Case of Security Risks

If a subscriber detects or suspects that their private key, PIN code, or mobile application has been exposed, compromised, copied, or misused, they must immediately notify the Issuer CA or RA using the communication methods provided as Revocation Contact in the Policy Management section of this CPS.

Upon receiving such a notification, Issuer CA or RA must re-verify the ownership of the affected digital certificate. Only after successful verification will the certificate revocation request be processed and approved.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application?

Digital certificates may be requested by the following entities:

- Individuals or organizations that meet the legal requirements and the conditions set forth in this Certificate Practice Statement (CPS) and have a legitimate need to use a digital certificate.
- The legal representative of an organization, provided they are legally authorized and meet the conditions specified in the applicable laws and CPS.

All certificate issuance requests are subject to review, validation, and authorization by the RA, who must verify compliance with the procedures and regulations established in this CPS.

4.2 Enrollment

Incode, through its Issuer Cas and RAs, is responsible for conducting the identity verification process, designed to prevent identity fraud and impersonation, for each digital certificate applicant in accordance with this CPS, prior to issuing the corresponding certificate.

1. Subscriber's Responsibilities

Subscribers, as part of the application process, they must:

- Complete the registration and identity verification process.
- Provide complete and truthful information in all required sections.
- Acknowledge responsibility for the accuracy of the submitted data and compliance with the applicable policies.

2. Registration Authority (RA) Review and Validation

The Issuer CA or RA are responsible for:

- Validating the subscriber's registration information and verifying their identity.

- Deciding whether to accept or reject the digital certificate application based on the verification results.

3. Issuance Process Upon Approval

If the application is accepted, the RA must:

1. Register the subscriber's information in the QTSP's digital certificate issuance system.
2. Submit the issuance request to the QTSP, which will proceed with generating and issuing the digital certificate.
3. Issue the certificate and perform the remote digital signature process.

4.3 Certificate Application Processing

4.3.1 Identification and Authentication Process

Identification and authentication is performed as described in section3.2.

4.3.2 Accept or refuse to issue digital certificates

4.3.2.1 Conditions for Certificate Issuance

Incode will only approve a digital certificate request if all of the following conditions are met:

- Successful verification of all identity and information details related to the digital certificate applicant.
- Full payment of all applicable fees for certificate issuance, digital signature services, and digital signature authentication under the remote digital signature model.

4.3.2.2 Conditions for Certificate Request Rejection

Incode will reject a digital certificate request under any of the following circumstances:

- Identity authentication failure for any required information about the applicant.
- Incomplete submission of the necessary documents required for certificate issuance.
- Lack of response from the applicant to a contact request within the specified time limit.

- Non-payment of the required fees for digital certificate issuance.
- Valid concerns regarding trust or reputation, where issuing a digital certificate to the applicant may negatively impact Incode's credibility or reliability.

This process ensures that only verified and legitimate applicants receive digital certificates, maintaining the integrity, trust, and security of the Incode's certification services.

4.3.3 Processing time for a certificate request

Incode is responsible for processing digital certificate applications in a timely manner.

However, there is no fixed time limit for completing the processing of a certificate application unless:

- A specific timeframe is established in the contract with the subscriber.
- A mutual agreement between the parties involved in the QTSP service specifies a timeframe.
- The certificate is issued for a remote signature, where it must be delivered just-in-time to complete the process.

This ensures flexibility in processing while allowing for contractual commitments where applicable.

4.4 Issuance of certificates

4.4.1 Actions performed by the CA during the issuance of the certificate

Once the identity of the applicant is successfully validate and approved, the CA proceeds with the certificate issuance process. This involves generating and signing the certificate while ensuring it meets security, compliance, and policy requirements.

Although the certificate request contains applicant-provided information, Incode may modify certain details based on pre-configured certificate profiles. These predefined profiles ensure:

- Certificates follow consistent formats and security parameters.
- Certificates align with CPS guidelines.
- Adjustments enforce key length requirements, cryptographic standards, and certificate extensions.

Common pre-defined certificate profile adjustments include:

1. Issuer Information. Incode CA sets the Issuer DN to reflect its own identity.
2. Key Usage & Extended Key Usage (EKU). Ensures the certificate is restricted to authorized functions (e.g., digital signatures, server authentication).
3. Certificate Validity Period. May be overwritten to conform with regulatory or policy limits.
4. Serial Number Assignment. Incode assigns a unique serial number for tracking and verification purposes.
5. CRL & OCSP Distribution Points. Incode embeds links to CRLs and OCSP responders.

4.4.2 Notifications to the subscriber or applicant of the certificate

Incode notifies the user once their digital certificate has been successfully created and provides access for the user to verify its availability. The valid certificate will be made available to the subscriber or accessible for download at the completion of the issuance process.

For One-Time or Short-Term certificates used for remote digital signatures, no notifications will be sent.

4.5 Acceptance of the certificate

4.5.1 Conducts constituting certificate acceptance

The subscriber confirms acceptance by:

- Explicit acceptance through email confirmation or digital acceptance mechanism.
- Implicit acceptance, which may occur if the subscriber uses the certificate for its intended purpose (e.g., signing a document, performing authentication).
- Fifteen calendar days have passed since the certificate issuance.
- For remote digital signature processes, acceptance is confirmed before the signing process, so no further action is required.

If the subscriber identifies any errors or inconsistencies in the issued certificate, they must:

- Reject the certificate and notify Incode for correction.
- Request revocation if an error is detected after issuance.
- Incode must then validate the issue and proceed with revocation and reissuance if necessary.

4.5.2 Publication of QTSP 's certificate

Once the QTSP receives acceptance of the issued digital certificate, Incode publishes the valid certificate in its online repository. All valid certificates are stored and accessible through:

- The web-based archive, where users can verify issued certificates.

4.6 Key Pair and Certificate Usage

4.6.1 Using the subscriber's certificate and private key

1. Private Key Activation Upon Certificate Acceptance
    - The use of the private key corresponding to the public key in the digital certificate is only permitted once the subscriber has accepted the certificate.
    - Until acceptance, the private key cannot be legally or operationally used.
2. Legal and Contractual Compliance

The digital certificate must be used strictly in accordance with:

- The Service Agreement terms.
- The policies outlined in this CPS.
- Applicable legal and regulatory provisions governing certificate usage.

3. Key Usage Restrictions
    - The usage of the digital certificate must align with the KeyUsage field specified within the certificate.
    - If a particular KeyUsage value is missing, the certificate cannot be used for that purpose.
        - Example: If the Digital Signature value is not present, the certificate cannot be used for digital signing.
4. Subscriber Responsibilities
    - The subscriber is responsible for protecting the private key from unauthorized access, loss, or misuse.
    - The private key must not be used if:
        - The digital certificate has expired or been revoked.
        - The digital signature and authentication service package has expired, as defined in the service contract.
5. X.509 Certificate Compliance
    - X.509 Version 3 certificates are generated in full compliance with RFC 5280.

- The Key Usage extension in X.509 v3 certificates is configured as follows:
  - Critical key fields are set to TRUE for essential certificate functions.
  - For end-user registrant certificates, some key fields may be enabled (TRUE) or disabled (FALSE) based on policy requirements.

		CAs	**Digital certificates for individuals and organizations**
Criticality		TRUE	FALSE
0	digitalSingnature	Clear	Set
first	nonRepudiation	Clear	Set
2	keyEncipherment	Clear	Set
3	dataEncipherment	Clear	Set
4	keyAgreement	Clear	Clear
5	keyCertSign	Set	Clear
6	CRLSign	Set	Clear
7	encipherOnly	Clear	Clear
8	decipherOnly	Clear	Clear

The subscriber has full control over all actions related to the private key, including: generation of secret key, generation of request for digital certificate, digital signature.

4.6.2 Relying party public key and certificate usage

Relying parties must independently evaluate digital certificates issued by Incode to ensure their validity and reliability before use. This evaluation includes the following verification steps:

1. Verify Certificate Issuance by Incode
   - Confirm that the digital certificate was issued by Incode's trusted certification chain.

2. Check Certificate Revocation Status
   - Ensure that the digital certificate has not been revoked by checking the latest CRL or querying the OCSP service.
3. Confirm Key Usage Compliance
   - Verify that the certificate is being used in accordance with the KeyUsage field extension defined in the certificate.
     - Example: If the KeyUsage field does not allow digital signatures, the certificate must not be used for signing documents.
4. Ensure the Certificate is Used for Its Intended Purpose
   - The relying party must confirm that:
     - The certificate is being used only for its approved and intended purposes.
     - The certificate usage is not prohibited or restricted under the CPS.
5. Verify the Status of the Entire Certificate Chain
   - The relying party must check the status of the digital certificate and all CAs involved in issuing it.
   - If any certificate in the certificate chain is revoked, the relying party must:
     - Assess the trustworthiness of any digital signatures created before revocation.
     - Acknowledge that continuing to trust a revoked certificate poses a risk.

4.7 Certificate Renewal

Certificate renewal allows a subscriber to extend the validity of their digital certificate before it expires, ensuring uninterrupted use of cryptographic functions such as authentication, encryption, and digital signatures.

When a digital certificate is renewed, a new key pair is generated to enhance security and cryptographic integrity.

Incode prefers re-keying over simple renewal, meaning that instead of renewing the certificate using the existing key pair, a new key pair is created for the renewed certificate.

4.7.1 Renewal Eligibility and Conditions

A digital certificate is eligible for renewal if:

- The existing certificate is still valid (not expired or revoked).
- The subscriber's identity details have not change.
- The renewal request is **submitted within the allowed renewal window** (90 days before the expiry date of the certificate).

A digital certificate is not eligible for renewal if:

- The certificate has already expired or been revoked, a new certificate application is required instead of renewal.
- If the certificate was issued as One-Time or Shor-Term certificate.

4.7.2 Processing requests for renewal of digital certificates

All certificate renewal requests are processed as certificate re-keys, following the procedures outlined in Section 4.7. This means that instead of simply extending the validity of an existing certificate with the same key pair, a new key pair is generated, and a new certificate is issued with an updated validity period.

4.7.3 Notice to subscribers about the issuance of new digital certificates

Notifications to the subscribers about the renewal is complete in accordance with re-key process describe in Section 4.4.

4.7.4 Terms of accepting renewal of digital certificates

The conditions governing the renewal of digital certificates are outlined in Section 4.4 and must be adhered to as part of the renewal process.

4.7.5 Announcement of extended digital certificates

Issuer CA or RA is responsible for publishing the renewed digital certificate on the public repository.

4.8 Certificate Re-Key

Comply with section 3.10

4.8.1 Who may request certificate re-key?

Only the certificate subscriber is authorized to request a re-key for the certificate. The request must follow the same procedure as the initial certificate application.

4.8.2 Processing new key requests for certificates

Issuer CA, RA and CA will treat certificate re-key as the initial certificate application.

4.8.3 Notice of release of new certificates to subscribers

Comply with section 4.4.2

4.8.4 Notice of acceptance of new issuance of certificate keys

Comply with section 4.5.1

4.8.5 Issuing a certificate that has been issued with a new key of QTSP

Comply with section 4.5.2

4.8.6 Notice of issuance of certificates of QTSP to other entities

Comply with section 4.5.3

4.9 Certificate modification

Certificate modification request are processed as initial certificate application.

4.9.1 Cases of modifying certificates

A digital certificate cannot be modified. Instead, the old certificate must be revoked, and a new key pair must be generated. The request to update certificate contents must be processed as a new certificate issuance with the newly generated key pair.

Revocation of the existing certificate is conditional on the issuance and acceptance of the new certificate. Therefore, the old certificate remains valid

until the new certificate is successfully issued and accepted. Only after acceptance of the new certificate will the previous certificate be revoked to ensure continuous availability and security.

4.9.2 Subject of request for certificate modification

Do not apply

4.9.3 Certificate modification request processing

Do not apply

4.9.4 Notice of release of new certificates to subscribers

Do not apply

4.9.5 Conditions for accepting subscription modifications

Do not apply

4.9.6 Issuance of modified certificates from QTSP

Do not apply

4.9.7 Notice of issuance of certificates of QTSP to other entities

Do not apply

4.10 Certificate Revocation and Suspension

4.10.1 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.

4.10.1.1 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.

4.10.1.2 Procedure for requesting revocation of certificate

Standard Revocation Request

- The subscriber 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 subscriber 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.

4.10.1.3 Revocation request grace period

If there is suspicion of key compromise or any other revocation reason outlined in Section 4.10.1, the subscriber 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.

Once the revocation request is processed, the CA is responsible for promptly updating the certificate's status in the CRL and OCSP services.

The CA follows the principles defined in this Certificate Practice Statement (CPS) to ensure the revoked certificate is properly announced and accessible to relying parties.

4.10.1.4 Time within which CA must process the revocation request

- Incode processes revocation requests within a reasonable timeframe, ensuring timely updates to certificate status.
- There are no specific time requirements for processing revocation requests unless explicitly agreed upon with the Subscriber in the service agreement.

- Once processed, the revoked certificate is updated in the CRL and OCSP services.

4.10.1.5 Mechanisms for Relying Parties to Check Certificate Status

Before using a digital certificate, the receiving party (relying party) must verify its status using the most recent Certificate Revocation List (CRL) or an equivalent validation mechanism.

Incode provides the necessary information to check certificate status via CRL and OCSP services.

Relying parties responsabilities

- Relying parties must use one of these mechanisms to verify the certificate's status before trusting it.
- OCSP is the preferred method for real-time validation, ensuring immediate revocation status updates.
- CRLs serve as an alternative when real-time verification is not required, offering batch revocation information.
- Failure to check a certificate's status may lead to security risks, such as trusting a revoked or compromised certificate, potentially exposing the relying party to fraud, data breaches, or compliance violations.

4.10.1.6 Frequency allocation CRL

The Certificate Revocation List (CRL) is issued and updated at regular intervals to ensure timely and reliable certificate status verification. Incode issues updated CRLs at least once a day.

4.10.1.7 Maximum Latency Between CRL Generation

- A new CRL shall be generated at least every 24 hours for end-entity certificates.
- CRLs for CA certificates shall be issued at least every 12 months or upon certificate revocation.

4.10.1.8 OCSP Availability

Incode OCSP responder is operational 24/7 to provide uninterrupted access to certificate status information. OCSP responses are signed digitally to ensure integrity and authenticity.

4.10.1.9 Online revocation status check requirements

Relying parties must verify the revocation status of a certificate before using it to ensure trust, security, and compliance.

4.10.1.10 Other forms of revocation advertisements

Do not apply

4.10.2 Certificate Suspension

Incode does not offer certificate suspension. If a certificate is no longer needed, compromised, or requires replacement, it must be revoked rather than suspended. Once revoked, the certificate cannot be reinstated and a new certificate must be issued if necessary.

4.11 Certificate Status Service

4.11.1 Operational characteristics

The certificate status is published in the public repository of Incode and are made available through the CRL and OCSP directories.

4.11.2 Service availability

The certificate status verification service (OCSP and CRL distribution) is available 24/7 to ensure continuous access for relying parties.

However, service availability may be affected by:

- Scheduled maintenance activities, which are announced in advance to minimize disruption.
- Unforeseen network outages due to factors beyond the control of Incode, such as cloud service provider disruptions.

If the certificate status service is temporarily inaccessible, relying parties should:

- Retry the request after a short interval.

- Use an alternative validation mechanism if available.
- Assess the risk before proceeding with certificate-based transactions.

The QTSP is committed to minimizing downtime and ensuring high availability of certificate status services.

4.11.3 Optional features

Do not apply.

4.12 End of subscription

Subscribers may terminate their contract for using the Incode's certificate services under the following conditions:

- Certificate Expiration Without Renewal
  - If the subscriber allows their certificate to expire without requesting a renewal, the contract for the certificate service automatically terminates at the end of the certificate's validity period.
- Voluntary Certificate Withdrawal Without Replacement
  - If the subscriber requests revocation or withdrawal of their certificate before it expires and does not apply for a replacement, the contract is considered terminated upon revocation..

4.13 Key scrow and recovery

Incode does not provide a key scrow and recovery services.

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 Key Changeover

Incode CA key changeover must be executed when the expiration date of the current CA keys approaches.

CA operators must ensure that no certificate is issued with an expiration date beyond that of the issuing CA.

In this regard, once the remaining validity period of the CA's keys is two years or less, the necessary procedures for generating a new key pair must be initiated. The current CA and the certificates it has issued will remain valid and in effect until the CA's expiration date.

5.7 Compromise and Disaster Recovery

5.7.1 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.

5.7.2 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.

5.7.3 The ability to maintain business continuity after a disaster

Incode ensures security measures are in place for the development, testing, and maintenance activities of Certification Authorities (CAs) and Registration Authorities (RAs). 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 system will support at least the following core PKI functions:
    - Issuance of digital certificates
    - Certificate revocation
    - Publication of revocation information
    - Key recovery support for enterprise customers using PKI management infrastructure
- The disaster recovery database is regularly synchronized with the production database to ensure data consistency.

5.8 CA or RA Termination

The termination of a CA or RA 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 Generate key pair and settings

6.1.1 Generate key pair

1. QTSP Key Pair Generation
    - The QTSP key pair is generated by the authentication authority on air-gapped computers (not connected to any network) to ensure maximum security and isolation.
    - 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 its own key pair, which is a self-signed certificate.
        - 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.

6.1.2 Transfer the secret key to the subscriber

Incode CA does not transfer or provide private keys to subscribers when issuing One-Time or Short-Term certificates. These certificates are designed for single-use or limited-duration digital signing, and the private key remains securely managed within the QTSP's trusted infrastructure.

For Long-Term certificates, the key pair will be made available for download at the end of the identity verification process, once the subscriber's identity has been successfully verified..

6.1.3 Transfer the public key to the certificate authority

Incode can process certificate issuance requests based on a Certificate Signing Request (CSR) in PKCS#10 format or certificate packets transmitted within an SSL-secured session..

6.1.4 Transfer CA's public key to trusted partners

Root CA and Issuer CAs digital certificates (containing the public key) are delivered to the subscriber via an online transaction through the CA's web server. Additionally, these certificates can be downloaded from the trusted repository for verification and use..

6.1.5 Key size

Key pairs must be of sufficient cryptographic strength to prevent the private key from being compromised during use. Incode system supports key lengths up to 8192 bits for RSA.

The current QTSP standard requires a minimum key length of 2048 bits for RSA keys. Certificates with key lengths of 1024 bits or lower are not accepted due to security vulnerabilities.

For its operations, Incode's CA must issue certificates using the following key sizes, signature algorithms, and hash algorithms.

	Key Size (At least)	Signature algorithm	Hash algorithm (At lesast)
Root CA	4096	RSA	SHA-256
Issuer CA	4096	RSA	SHA-256
Timestamp Authority	4096	RSA	SHA-256
OCSP Signer	4096	RSA	SHA-256
End-user certificate	2048	RSA	SHA-256

6.1.6 Generate parameters for the public key and check the quality

No regulations.

6.1.7 Key use purpose (as in X.509 v3 key usage field)

The Key Usage extension in X.509 v3 certificates defines the intended purposes of the cryptographic key pair, ensuring that the certificate is used only for its designated functions.

6.1.7.1 Root CA – Self-signed certificate

Root Certificates hold the highest level of trust in a PKI and must be protected from unnecessary use. To maintain security, integrity, and compliance, the use of these private keys is strictly limited to the following scenarios:

- The Root CA must sign its own certificate to establish trust in the PKI hierarchy.
- The Root CA can sign certificates for Subordinate CAs, allowing them to issue end-entity certificates.
- The Root CA may issue certificates to secure internal administrative operations, including:
    - CA operational roles (e.g., administrators, cryptographic officers).
    - Internal CA system devices used for critical PKI functions.
- The Root CA may issue certificates for OCSP responders, enabling certificate status validation in real-time.

6.1.7.2 Suscriber certificates

The Key Usage extension in subscriber certificates defines the intended cryptographic functions that the private key associated with the certificate can perform. This ensures that the certificate is used only for its designated purposes

and helps maintain compliance and security within the Public Key Infrastructure (PKI).

The following key usage attributes are commonly assigned to subscriber certificates, depending on their purpose:

1. Digital signature
2. Content Commitment (Non-repudiation)
3. Key Encipherment
4. Data Encipherment
5. Key Agreement

6.2 Protect the secret key and control the encryption method

6.2.1 Cryptographic module standards

Incode CA system utilizes specialized FIPS 140-2 level 3 HSMs that comply with the standards issued by the Ministry of Information and Communications and are operated according to the manufacturer's guidelines.

These HSMs handle all key management operations, including:

- Key generation
- CA key management
- Digital certificate signing
- Validation
- Secure key storage and backup

All key-related operations are performed exclusively within the HSM, ensuring that private keys are never exposed and cannot be accessed by unauthorized individuals.

6.2.2 Multiple secret key control

Incode implements a multi-control rule to protect the activation data of the CA private key. This ensures that sensitive cryptographic operations require the participation of multiple trusted individuals.

Participation in this process is validated through a quorum-based authentication mechanism, where a threshold number of quorum tokens (n) out of a total (m) must be presented to approve key activation, signing, or recovery operations.

No single individual has full control over key access or cryptographic functions, ensuring compliance with FIPS 140-2/140-3 Level 3 security standards and enhancing security, integrity, and regulatory compliance.

6.2.3 Private key scrow

Incode does not scrow private keys.

6.2.4 Private key backup

The HSMs implemented by Incode's CA as part of its PKI infrastructure have automated backup procedures, executed every 24 hours or whenever the HSM cluster is modified.

All backups are encrypted and can only be restored if the request originates from the security group under which they were generated, ensuring controlled and authorized recovery.

Private key backups are protected with the same security measures as active keys, guaranteeing confidentiality, integrity, and compliance with industry standards.

Incode backs up CA private keys for disaster recovery and restoration purposes, ensuring business continuity and operational resilience.

No backups are made for suscribers private eys.

6.2.5 Private key archival

When a QTSP certificate expires, the CA key pairs associated with the certificate are securely stored for a minimum period of five (5) years in hardware modules

equipped with strong encryption mechanisms, ensuring compliance with the requirements of this CPS.

These CA key pairs will not be used for any signing operations after expiration, unless the CA certificates are officially restored under the provisions outlined in the CPS.

6.2.6 Private key storage on cryptographic modules

Incode Root CA and Issuer CA certificates are stored in a HSM that is certified at least in FIPS 140-2 level3.

6.2.7 Private key activation

Private key activation procedure is described in Section 6.1.1. Once key activation is complete, the key remains active for an indefinite period, unless explicitly deactivated or revoked according to security policies

6.2.8 Private key deactivation

Do not apply.

6.2.9 Private key destruction

Subscribers to whom the certificate was issued are fully responsible for the destruction of their private key.

For One-Time or Short-Term certificates intended for document signing, the private key is destroyed immediately after the signing process is complete. These certificates are never stored on any device.

The private keys of Root CA and Issuer CAs are securely destroyed within the HSM using a zeroization process, ensuring that no residual data remains and that the keys cannot be recovered.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Incode stores and maintain all of the public keys issued by its Root CA and Issuer CAs.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Certificate type	Max validity period
Root CA	25 years
Issuer CA	15 years
OCSP Responder	2 years
Timestamp Authority	5 years
Qualified certificates	Up to 4 years
Qualified One-Time or Short-Term Certificates	Duration of the signing transaction

6.4 Computer security control

6.4.1 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.

6.4.2 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.

6.5 Life Cycle Security Controls

6.5.1 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.

6.5.2 Security Management Control

Incode implements mechanisms and policies to control, monitor, and maintain the configuration of its PKI infrastructure.

6.5.3 Security control over a lifecycle

No stipulation.

6.6 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.

6.7 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 Format of Certificates, CRL and OCSP

7.1 Certificate Profile

A certificate profile defines the structure, attributes, and extensions of a digital certificate, specifying how it should be used within a Incode PKI. It ensures compliance with standards such as X.509 v3, defining necessary fields and constraints based on the certificate's purpose.

Standard and Mandatory Certificate Fields

Field	Description
Version	Defines the X.509 version
Serial Number	Unique identifier for the certificate
Signature Algorithm	Cryptographic algorithm used for signing
Issuer	Identifies the CA that issued the certificate
Validity Period	Defines the start and expiration dates of the certificate (Not Before / Not After)
Subject	Entity (organization, individual, or device) to whom the certificate is issued
Subject Public Key	The subscriber public key

7.1.1 Version

Qualified certificates issued by Incode are Version 3 – X.509 certificates.

7.1.2 Certificate extension

Incode certificates support extensions defined in RFC 5280, allowing additional metadata to be included in certificates for enhanced security, validation, and policy enforcement. These extensions provide crucial information about key usage, subject identification, certificate policies, and revocation mechanisms.

Each extension consists of:

- OID (Object Identifier). Unique identifier for the extension.
- Critical Flag. Determines whether the extension must be processed by relying parties.
- Value. Encoded data providing specific extension details.

Extension Name	OID	Critical?	Purpose
Basic Constraints	2.5.29.19	Yes (for CA)	Defines if the certificate is a CA certificate and limits the certificate chain depth.
Key Usage	2.5.29.15	Yes	Specifies allowed cryptographic operations
Extended Key Usage (EKU)	2.5.29.37	No	Specifies additional intended certificate uses
Subject Key Identifier (SKI)	2.5.29.14	No	Provides a unique identifier for the certificate's public key.
Authority Key Identifier (AKI)	2.5.29.35	No	Links a certificate to its issuing CA by referencing the CA's key identifier.
Certificate Policies	2.5.29.32	No	Specifies policies under which the certificate was issued.
Policy Constraints	2.5.29.36	No	Specifies constraints on certificate policies in the chain.
Name Constraints	2.5.29.30	Yes (for CA)	Restricts subject names allowed in the certificate hierarchy.
Subject Alternative Name (SAN)	2.5.29.17	No	Lists alternative identities for the certificate

Extension Name	OID	Critical?	Purpose
Issuer Alternative Name	2.5.29.18	No	Lists alternative identities for the issuing CA.
CRL Distribution Points (CDP)	2.5.29.31	No	Provides a URL where the CRL can be retrieved.
Authority Information Access (AIA)	1.3.6.1.5.5.7.1.1	No	Provides the OCSP responder URL or issuing CA information.
OCSP No Revocation Checking	1.3.6.1.5.5.7.48.1.5	No	Indicates that the certificate should not be checked for revocation via OCSP.
Inhibit AnyPolicy	2.5.29.54	Yes (for CA)	Restricts the use of the anyPolicy OID in the certificate chain.

7.1.3 Algorithm number

Certificate algorithms are identified using Object Identifiers (OIDs), which specify cryptographic algorithms for digital signatures, hashing, and key management in X.509 certificates. These OIDs ensure standardization and interoperability across different PKI implementations.

Algorithms use by Incode, include:

RSA Algorithms:

Algorithm	OID
sha256withRSAEncryption	{iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }

ECSDA Algorithms

Algorithm	OID
ecdsa-with-SHA224	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA224(3) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA256(3) 2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA384(3) 3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA512(3) 4}

7.1.4 Name Form

Incode RootCA, Issuers CAs, RAs and Subscriber (end-entity) are identified using Distinguished Names (DNs) as per RFC 5280. The CA name appears in the Issuer field of certificates and typically includes the Common Name (CN), Organization (O), Country (C), and optionally State (ST) or Email (E).

The Subscriber name, found in the Subject field, must accurately represent the certificate holder—whether an individual, an organization, or a server (e.g., "CN=www.example.com").

7.1.5 Name constraints

There are no constraints other than specified.

7.1.6 Certificate Policy OID

Incode includes an Object Identifier (OID) in each issued certificate, specifying the certificate policy under which it was issued. The OID uniquely identifies the applicable policy and ensures compliance with the related CPS. The OIDs covered by this CPS are detailed in Section 1.2 of this document.

7.1.7 Usage of binding policy extension

Do not apply

7.1.8 Semantic handling for the extension of important certificates

Do not apply

7.2 CRL Profile

Incode will create and publish a CRL X.509 version 2 that complies to RFC 5280.

Version	V2
Signature Algorithm	Signature algorithm is inherited from CA.
Issuer	Incode CA
Effective date	Indicate the date and time the CRL was published
Next Update	Indicate the date and time when the next CRL will be published.
Revoked Certificates	serialNumbers of revoked certificate

Certificates that have been revoked by Incode are recorded in the Certificate Revocation List (CRL). Each entry identifies the revoked certificate by its serial number and revocation date, which specifies the exact time and date when the certificate was officially revoked by the Certification Authority (CA).

7.2.1 Version

Incode will create and publish a CRL X.509 version 2 certificate revocation list.

7.2.2 CRL and CRL entry extensions

CRLs must use CRL extensions that comply with RFC 5280. The following extensions may be included in a CRL:

- Reason Code – Specifies the reason for certificate revocation.
- Invalidity Date – Indicates the date when the certificate was deemed invalid.

If a reasonCode extension is present in a CRL entry, it must specify the most appropriate reason for the certificate's revocation.

Special Case for CA Certificate Revocation:

- If a CA certificate is revoked, the reasonCode cannot be set to "unspecified" (0). In such cases, the reasonCode extension must be omitted entirely.

No Certificate Suspension Policy:

- Since Incode does not offer certificate suspension, the certificateHold (6) reasonCode cannot be used.

If multiple revocation reasons apply, the certificate must be revoked using the most appropriate reason code, following a defined order of preference.

Reason Code	Value	Description
unspecified	0	Revocation reason not specified.
keyCompromise	1	The private key has been compromised.
cACompromise	2	The issuing CA's private key has been compromised.
affiliationChanged	3	The certificate holder's organization has changed.
superseded	4	The certificate has been replaced with a new one.
cessationOfOperation	5	The entity no longer requires the certificate.
certificateHold	6	The certificate is temporarily suspended.

Reason Code	Value	Description
removeFromCRL	8	The certificate was on hold but is now removed.
privilegeWithdrawn	9	The subject's rights to use the certificate have been revoked.
aACompromise	10	The key of an attribute authority (AA) has been compromised.

7.3 Profile of OCSP

OCSP follows the data structure described in the IETF RFC 6960 standard.

Version	V1
Responder ID	Name of OCSP requesting
Produced At	Release date
Responses	Status code (good, revoked, not known) of the request

7.3.1 Version

The OCSP profile uses version 1 in requests and responses as described in RFC 6960.

7.3.2 OCSP Extensions

Not determined yet

8 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.

8.1 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.

8.2 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.

8.3 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.

8.4 Subjects in the evaluation process

The audit scope and requirements vary depending on the entity being audited. Each entity must undergo regular performance audits as part of the annual review of its information systems and compliance with QTSP policies.

RA (Registration Authority) Audits:

- Subscribers that are businesses with proven compliance must undergo an annual audit.
- The RA is audited based on QTSP requirements to identify exceptions or non-compliance with QTSP policies.
- If non-compliance is detected, the RA must implement corrective actions to ensure compliance.

Incode and Related Party Inspections:

- The QTSP audit must be conducted by an independent entity that meets the following qualifications:
- Expertise in Public Key Infrastructure (PKI) technology.
- Proficiency in information security tools and techniques.

- Certification by the National Root CA to validate its authority.

8.5 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).

8.6 Result announcement

The CA Administration will publish the results on Incode website with detailed information about the result of the audit, including any CPS violation.

9 Other commercial and legal matters

9.1 Fees

9.1.1 Fee for issuance of Certificate or renewal of certificate

The cost of issuing or renewing a digital certificate issued by Incode's CA must be covered by subscribers, based on the fees defined in the commercial agreements established with each subscriber.

9.1.2 Fees for using certificates

Subscribers of QTSP and RA are not required to pay for the storage of certificates in an archive or for the service that provides online certificate information to trusted partners.

9.1.3 Fees for accessing information about certificate status and certificate revocation

Incode QTSP service participants are not charged for the issuance of CRLs or for accessing certificate revocation status information for digital certificates issued by Incode's CA.

However, while basic revocation status checks are provided free of charge, Incode may charge a fee for providing OCSP or other certificate status information services, especially if usage exceeds 1,000 queries per day.

9.1.4 Usage fees for other services

Subscribers can access this CPS free of charge through:

- https://psc.incode.com/qtsp-legal-repository/.

QTSP service participants are also not required to pay a fee for accessing the CPS.

However, the use of this document for purposes such as copying, redistributing, editing, or creating derivative works is subject to a legal agreement with the rights holder. Additionally, if any services beyond those mentioned are provided, the costs will be specified in the commercial agreement established with the subscriber.

9.1.5 Fee Refund Policy

A refund will only be provided to the subscriber if explicitly stated in the commercial agreement between Incode and the subscriber regarding the Qualified Electronic Signature (QES) service issued by Incode's Certification Authority (CA).

If no refund terms are specified in the agreement, Incode is not obligated to issue a refund for the service.

9.2 Financial responsibility

9.2.1 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.

9.2.2 Cases where QTSP conducts insurance compensation

QTSP provides insurance indemnification in the following cases:

- Errors caused by the CA, including technical failures occurring during the certificate issuance process, where the CA is directly responsible.
- Compensation will be provided in accordance with the terms and conditions specified in the contract with the subscriber.

9.2.3 Cases that are not covered by insurance

Incode is not responsible in the following cases:

- Use of certificates in violation of the provisions outlined in this CPS.
- Forgery of documents or fraudulent activities related to certificate usage.
- Improper device configuration or misuse of certificates that falls outside the CA's responsibility.
- Loss, tampering, or destruction of the private key by the subscriber.
- Loss or disclosure of the PIN code protecting the private key by the subscriber.
- Errors by the RA, including:
    - Authentication failures
    - Incorrect data identification
    - Certificate number mismatches
    - Incorrect public key values
    - Failure to send the correct certificate request

In cases where RA errors occur, the RA assumes full responsibility for the subscriber, and compensation will be handled according to the terms of the contract with the subscriber.

9.2.4 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.

9.3 Confidentiality of business information

9.3.1 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..

9.3.2 Information is not within the scope of the confidentiality process

The information issued in the digital certificate, CRL and OCSP is not considered confidential.

9.3.3 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.

9.4 Confidential personal information

9.4.1 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.

9.4.2 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.

9.4.3 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.

9.4.4 Responsibility to protect privacy

Incode and its accredited RAs are responsible for protecting the privacy of their subscribers and must comply with the privacy laws in their jurisdiction.

9.4.5 Notice and permission to use confidential information

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

9.4.6 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.

9.5 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.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Incode does not provide any warranties, guarantees, or assurances regarding its products or services, except as explicitly outlined in this CPS or in a legally binding agreement with its subscribers. Any descriptions, statements, or implied commitments that are not expressly stated in this CPS 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.

Incode Representations (as Specified in this CPS):

- The CA operates in full compliance with its CPS.
- The CA follows industry standards, including RFC 5280 and ETSI EN 319 411-2.
- The CA maintains and publishes a CRL and OCSP service to provide real-time certificate status information.
- The CA processes revocation requests promptly and ensures that revoked certificates are included in the next CRL update or OCSP response.
- The CA ensures that subscribers are properly informed of their rights, obligations, and responsibilities when using issued certificates.
- The CA is not responsible for misuse of certificates by subscribers or relying parties beyond the scope of the CPS.

Limitations of Liability:
Incode cannot guarantee that its services will be suitable for a subscriber's particular purpose or that the service will be error-free.

9.6.2 RA representation and warranties

RAs are responsible for performing the identification and authentication of certificate applicants in strict accordance with the procedures outlined in this CPS.

RAs are expected to:

- Conduct identity verification with due diligence, ensuring compliance with industry best practices and regulatory requirements.
- Apply appropriate security controls to prevent fraud, identity theft, or improper issuance of certificates.
- Maintain accurate records of all verification processes for auditing and compliance purposes.
- Act in accordance with legal and regulatory obligations governing identity verification in PKI environments..

However, no additional warranties or guarantees are provided beyond what is explicitly stated in this CPS.

9.6.3 Suscriber representation and warranties

When a subscriber requests Incode to issue a digital certificate, the subscriber agrees to accept, use, and protect the certificate and its associated private key in strict compliance with the provisions of the CPS in effect at the time of issuance.

Suscriber representations are:

- The subscriber is responsible for ensuring that the private key is stored securely and protected against unauthorized access, loss, or compromise.
- The certificate and private key must be used only for the purposes specified in the CPS and must not be shared or misused.
- If a subscriber loses or suspects that their private key has been compromised, they must immediately notify Incode to initiate certificate revocation.
- This ensures that the CA can take timely action to revoke the certificate, preventing further use and notifying relying parties to reject it.
- By requesting a certificate, the subscriber agrees to adhere to all provisions of the CPS, including its security policies, key management rules, and revocation procedures.
- Non-compliance with the CPS may result in mandatory certificate revocation by Incode to maintain security and trust in the PKI ecosystem.

No Additional Guarantees Required from the Subscriber:

- If a subscriber violates CPS requirements, QTSP reserves the right to revoke the certificate without requiring additional approval from the subscriber.

- The subscriber cannot demand additional warranties from QTSP regarding certificate validity once revocation has been requested or enforced.

9.6.4 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.

9.6.5 Representation of other stakeholders and guarantee matters

No stipulations.

9.7 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.

9.8 Limitation of Liability

- This CPS 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 CPS is held unenforceable by a trial or other competent hearing, the remainder of the CPS remains in force. effect.

9.9 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.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 The effect of the end and the harm

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

9.11 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.

9.12 Amendment

9.12.1 Amendment procedures

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

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

9.12.2 Cases where object identification (OID) modification is required

Changing the item in the CPS will change the OID. This decision is made by the CPS manager of Incode.

9.12.3 How and when to notify

QTSP reserves the right to determine whether a change to the CPS is necessary.

- QTSP collects and evaluates CPS change requests from participants in the QTSP service.
- If QTSP determines that a change is required, it will propose and implement the change, providing advance notice in accordance with this section.

Urgent Security Changes

If QTSP identifies a security risk that could compromise the QTSP service, it has the right to immediately modify the CPS without prior notice.

- Such changes take immediate effect upon publication.
- QTSP will notify all relevant parties as soon as possible after implementing the change.

Modification Period & Feedback

Non-urgent CPS modifications are subject to a 15-day review period from the date of publication in the QTSP service archive.

During this period, QTSP service participants may submit comments or objections before the modification period expires.

9.13 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.

9.14 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.

9.15 Compliance With Applicable Law

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

9.16 Mixed Terms

Do not apply.

9.17 Other provisions

Do not apply.