incode psc

PKI Disclosure Statement

Version	Modified by	Modifications made	Date modified
1.0	LV	Content	01/05/2025

Tabla de contenido

1. Overview

Purpose and scope of this document

This document serves as a comprehensive reference guide specifically designed for Subscribers and Relying Parties who utilize Qualified Certificates issued by Incode Czech Republic s.r.o. Its primary objective is to provide a concise and accessible summary of the essential information contained within the foundational documents that govern our qualified trust services:

1. **Incode CPS** which details the technical, procedural, and administrative practices employed in certificate lifecycle management

Intended audience

This summary is specifically tailored for:

- **Subscribers**: Organizations and individuals who have obtained Qualified Certificates from Incode for their digital signature and authentication needs.
- **Relying Parties**: Third parties who rely upon and accept the validity of Qualified Certificates issued by Incode in their business processes and legal transactions.

Document relationship and limitations

Important Legal Notice: This document functions exclusively as an informational summary and reference tool. It is essential to understand that:

- This summary does not substitute, supersede, or replace the legally binding provisions contained in Incode's General Terms and Conditions for Use of Qualified Trust Services
- This document does not modify or alter the technical specifications and procedures detailed in the Certificate Policy Statement (CPS).
- In the event of any discrepancy or conflict between this summary and the original governing documents, the full versions of the CPS shall prevail
- This summary is provided solely for the convenience of Subscribers and Relying Parties to facilitate understanding of key provisions and obligations

Recommended usage

While this document provides valuable insights into the most relevant aspects of our qualified trust services, users are strongly encouraged to:

- Consult the complete CPS for comprehensive understanding of all rights, obligations, and procedures
- Seek legal counsel when necessary to fully understand contractual implications
- Reference the original documents for any formal or legal proceedings

Contact Information

Incode Czech Republic, s.r.o.
Pujmanové 1753/10a, Nusle, 140 00 Prague 4
psc@incode.com, tsp@incode.com
https://psc.incode.com/eu
e-mail: info@incode.com
DataBox: 76gmkd8

Obligations of the 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.

Revocation

A Subscriber requesting revocation shall send a request to Incode by e-mail at revocations@incode.com. Incode will promptly initiate revocation of the certificate.

Certificate types

1. Qualified certificates for natural person for remote signature

Certificate status verification requirements for relying parties

Before accepting or relying upon any Qualified Certificate issued by Incode, Relying Parties have a fundamental obligation to verify the current validity status of the certificate. This verification is essential to ensure that the certificate has not been revoked, suspended, or otherwise compromised since its issuance.

Primary verification method: OCSP service
Alternative verification method: Certificate Revocation List (CRL)

Applicable CPS and other documents

Relevant agreements, policies and practice statements for the use of the certificates are:

1. Qualified Certificates Policy / Statement
2. Remote Signature Policy / Statement
3. General Terms and Conditions
4. Privacy Policy for Customers Personal Data

Current versions of all applicable documents are publicly available in the Incode repository at https://psc.incode.com/qtsp-legal-repository/

Previous versions of all applicable documents are publicly available in the Incode archive repository at https://psc.incode.com/qualified-tsp-regulatory-and-contractual-documents-archive/

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.

Privacy policy

Incode process personal data in accordance to the applicable data protection legislation in force. For further details, please refer to Incode Privacy Policy for Customers Personal data available at https://psc.incode.com/qtsp-legal-repository/

Limitation of Liability

1. Qualified Certificate service 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.
2. The liability of the parties is regulated and limited according to the signed contract.
3. 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.

Disclaimer of warranties

1. The CA does not warrant that its certificate issuance, validation, or revocation services will be uninterrupted, error-free, or continuously available.
2. Service availability may be affected by technical failures, scheduled maintenance, or force majeure events.
3. The CA makes no warranty that its certificates or services will be fit for any particular purpose beyond those explicitly outlined in this CPS.
4. Subscribers and relying parties are responsible for evaluating the suitability of certificates for their intended use.
5. All certificates and any related software and services are provided “as is” and “as available”
6. To the extent permitted by law, subscription contracts and trust partner contracts may refuse QTSP's guarantee.

Council Law

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

1. The relevant national legislation governing Incode operations
2. The Czech Republic’s e-commerce laws

All disputes arising from:

1. The terms and provisions of this CPS
2. The activities of the CA and RA
3. The use of QTSP services
4. 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.