PUBLIC

# Insta Trust Services

## Management of Remote Qualified Seal Creation Device

## Trust Service Practice Statement

---

| | | | |
|---|---|---|---|
| **Status** | Published | **Doc. No.** | D91014SD41 |
| **Version** | D | **Pages** | 20 |
| **Updated** | 2026-10-23 | | |

Copyright © 2026 Insta Advance Oy

# Administrative Information

## Document Control

| | Name | Signature | Date |
|---|---|---|---|
| **Author** | Insta Advance | | 2026-10-23 |
| **Inspected by** | Insta Advance | | 2026-10-23 |
| **Approved by** | CS Steering Group | | 2026-10-23 |
| **Archive ref** | | | |

## Version History

| Ver-sion | Description | Changed by | Date of change |
|---|---|---|---|
| A | Published | ViK | 2026-05-15 |
| B | Published | ViK | 2026-06-15 |
| C | Published | ViK | 2026-08-17 |
| D | First public version | JaL | 2026-10-23 |
| | | | |
| | | | |


Copyright © 2026 Insta Advance Oy

# Table of Contents

**Administrative Information** ..... **2**

**Table of Contents** ..... **3**

**1 Introduction** ..... **5**
1.1 Scope ..... 5
1.2 Standards conformity ..... 5
1.3 Definitions and abbreviations ..... 5
1.4 Overview ..... 7
1.5 References ..... 7

**2 Risk Management** ..... **8**

**3 Policies and practices** ..... **9**
3.1 Trust Service Practice Statement ..... 9
3.2 Terms and Conditions ..... 9
3.3 Obligations of all external organizations ..... 9
3.4 Information and Network Security Policy ..... 9

**4 TSP Management and Operations** ..... **11**
4.1 Internal organization ..... 11
4.1.1 General ..... 11
4.1.2 Organization reliability ..... 11
4.1.3 Segregation of duties ..... 11
4.2 Human resources ..... 11
4.3 Asset management ..... 11
4.3.1 General ..... 11
4.3.2 Assets classification ..... 12
4.3.3 Asset handling and storage media ..... 12
4.4 Access control ..... 12
4.4.1 General ..... 12
4.4.2 Privileged and system administration accounts ..... 12
4.4.3 Administration systems ..... 12
4.4.4 Identification ..... 12
4.4.5 Authentication ..... 13
4.4.6 Multi-factor authentication ..... 13
4.5 Cryptographic controls ..... 13
4.6 Physical and environmental security ..... 13
4.7 Operation security ..... 13
4.8 Network security ..... 13
4.9 Vulnerabilities and Incident management ..... 14
4.9.1 Monitoring and logging ..... 14
4.9.2 Incident response ..... 14
4.9.3 Reporting ..... 14


Copyright © 2026 Insta Advance Oy

4.9.4 Event assessment and classification ..... 14
4.9.5 Post-incident reviews ..... 14
4.10 Collection of evidence ..... 14
4.11 Business continuity management ..... 15
4.11.1 General ..... 15
4.11.2 Backup ..... 15
4.11.3 Crisis management ..... 15
4.12 TSP termination and termination plans ..... 15
4.13 Compliance ..... 15
4.14 Supply chain ..... 16
4.14.1 Supply chain policy ..... 16
4.14.2 Responsibility, third party agreements and SLA ..... 16

**5 SSAS Practice Statement ..... 17**
5.1 Policy claims ..... 17
5.2 Publication and repository responsibilities ..... 17
5.3 Signing key initialization ..... 17
5.3.1 Signing key generation ..... 17
5.3.2 eID means or identity linking ..... 17
5.3.3 Certificate linking ..... 18
5.3.4 eID means provision ..... 18
5.4 Signing key life-cycle operations ..... 18
5.4.1 Signature activation ..... 18
5.4.2 Signing key deletion ..... 19
5.4.3 Signing key backup and recovery ..... 19
5.5 Additional facility, management, and operational controls ..... 20
5.5.1 Audit logging procedures ..... 20
5.5.2 Records archival ..... 20
5.5.3 Compromise and disaster recovery ..... 20
5.5.4 SSASP service termination ..... 20


Copyright © 2026 Insta Advance Oy

# 1 Introduction

## 1.1 Scope

This document describes the practices applied by Insta Advance for the provisioning of Qualified Trust Service Provider (QTSP) services operating a remote Qualified electronic Signature/Seal Creation Device (QSCD).

Insta Advance Oy (Insta):

- Enterprise number: 1597850-3
- Address: Sarankulmankatu 20, 33900 Tampere, Finland

## 1.2 Standards conformity

This practice statement claims conformity with

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers and
- ETSI TS 119 431-1 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev.

## 1.3 Definitions and abbreviations

| | |
|---|---|
| eIDAS regulation | Regulation (EU) no 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC |
| eIDentification Means | Electronic identification means as per the eIDAS regulation |
| SSA | The Server Signing Application offering from Insta |
| Relying party | Natural or legal person that relies upon the electronic signature |
| Subscriber | Legal or natural person bound by agreement with DVV to any subscriber obligations. |
| Practice Statement | A statement of the practices that the TSP employs in providing a Trust Service |
| Subscriber Certificate | Public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the Certification Authority, which issued it |


Copyright © 2026 Insta Advance Oy

| | |
|---|---|
| Supervisory Body | The authority which is designated by member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state |
| CA | Certificate Authority |
| DDoS | A Distributed Denial-of-Service attack to disrupt normal traffic to a web property |
| DTBS/R | Data To Be Signed Representation |
| DVV | Digi- ja väestötietovirasto, Finland |
| eID | Electronic Identification |
| EUSPv2 | EU SSAS Policy |
| ISMS | Information Security Management System |
| OID | Object Identifier |
| PIN | Personal Identification Number |
| QSCD | Qualified Electronic Signature/Seal Creation Device |
| QTSP | Qualified Trust Service Provider |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SAD | Signature Activation Data |
| SAM | Signature Activation Module |
| SAP | Signature Activation Protocol |
| SCA | Signature Creation Application |
| SCDev | Signature Creation Device |
| SSA | Server Signing Application |
| SSAS | Server Signing Application Service |
| SSASP | Server Signing Application Service Provider |
| TSA | Timestamping Authority |


Copyright © 2026 Insta Advance Oy

| | |
|---|---|
| TSP | Trust Service Provider |
| URI | Uniform Resource Identifier |
| MOG | Maintenance Operation Guidance |

## 1.4 Overview

Insta acts as a Qualified Trust Service Provider for management of remote Qualified Sealing/Signature Creation Device for DVV electronic Seal/Signature Generation Service.

The current practice statement describes the practices and procedures that Insta implements to comply with the requirements of the eIDAS regulation and the Supervisory Body (Traficom).

Insta has ISO/IEC 27001 certified ISMS, which manages the information security of the services it provides, including this service. ISMS also takes into account eIDAS requirements.

## 1.5 References

| Reference | Document |
|---|---|
| Termination Plan - Seals | D91014SD43_1(TSP Termination plan Seals) |
| Insta Trust Services – Terms and Conditions | D91014SD46(Terms and Conditions) |
| ISO/IEC 27001 Certificate | Kiwa ISO/IEC 27001 Certificate |
| ISO9001 Certificate | Kiwa ISO9001 Certificate |
| FSC Certificate | Facility Security Clearance Certificate, NSA of Finland |


Copyright © 2026 Insta Advance Oy

# 2 Risk Management

Insta has implemented risk management processes in its ISMS. Risk assessment process includes identification, analyses and evaluation of the risk. Risk treatment process manages the risks with level above the defined threshold.

Risk identification is performed annually, and it is reviewed regularly during the year. Risks related to new services are assessed during the development cycle and services are not transferred into production phase until risk level is acceptable. Risk identification is done based on information gathered via threat intelligence, vulnerability analysis, security testing, and personnel surveys.

Risk analyses process evaluates the likelihood and impact of the identified risks in context of the Insta services. These produce the level of the risk. Risk management process defines threshold level to the risks that must be treated. Risk assessment is reviewed regularly during the year.

Risk treatment options are analyzed based on risk level, cost of the mitigation actions, and residual risk level. Once the best option is implemented, its effectiveness is regularly monitored.


Copyright © 2026 Insta Advance Oy

# 3 Policies and practices

## 3.1 Trust Service Practice Statement

The current Insta Trust Service Practice Statement is approved by Insta Cyber Security Unit Executive Steering Group.

The Insta Trust Service Practice Statement is made publicly available via Insta's website: https://www.insta.fi/en/cybersecurity/services/qtsp/.

Any change to the Trust Service Practice Statement leads to a new publication of the revised Insta Trust Service Practice Statement -document. Old versions of the Trust service Practice Statement will still be available on the same website.

Changes that have no impact on the Subscribers or Relying Parties will not be notified up front. Changes that impact Subscribers or Relying Parties and that do not impact the secure and compliant operation of the services will be notified via the Insta's website at least 2 weeks in advance of the implementation of the change or via direct contact.

In case of changes that impact Subscribers or Relying Parties that are urgent because they are required to maintain the security or compliance of the solution, a best effort will be performed to notify via the Insta's website or direct contact as soon as possible.

The present Practice Statement supports the provisioning of trust services that can reach the eIDAS qualified level. To achieve this level of service, this practice statement claims conformity with ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

## 3.2 Terms and Conditions

The Terms and Conditions of management of the remote QSCD are incorporated into Terms and Conditions of Electronic Seal/Signature Generation Service of the DVV.

## 3.3 Obligations of all external organizations

This service uses third party software supplier. Insta has agreed a license agreement with the supplier and has active maintenance and agreement support with the supplier-Supplier is bound by the general EU regulation and furthermore software is agreed to fulfil the eIDAS regulation regarding remote seal generation.

This service is used by a TSP providing electronic seal generation services. Insta has a service agreement which states the obligations for the parties. Both are operating under EU and Finnish regulation.

## 3.4 Information and Network Security Policy

The information and cybersecurity policy approved by the Insta board of directors outlines and guides the content of the Cyber Security business unit's ISMS. The information and cybersecurity policy includes:

- Description of the key stakeholders


Copyright © 2026 Insta Advance Oy

- Definition of  the objectives
- Definition of the factors that guide actions
- Definition of the principles of security
- Definition of the access and usage rights principles
- Definition of the organization
- Definition of security monitoring and possible sanctions
- Definition of the priority of security actions/tasks

Insta ISMS is managed by Insta Cyber Security Executive Steering Group. The scope of this ISMS applies to the provision of its core services to subscribers, i.e. the enrolment, share ID, sign up, login, confirm and signature services.

The scope includes physical locations, personnel, assets, data centers and ICT-equipment and software. It covers the management of information and business activities that support these services.

ISMS contain lower-level policies guides, practices, and procedures for various activities. Reviews and checks are performed on the above-mentioned documentation and configuration of the TSPs systems for continued compliance with Insta security policies and ISMS requirements. The frequency of execution depends on the type of review or check but are performed at least once a year.


Copyright © 2026 Insta Advance Oy

# 4 TSP Management and Operations

## 4.1 Internal organization

### 4.1.1 General

Insta implements ITIL -best practices for ICT-operations and is certified ISO/IEC 27001 and ISO9001.

### 4.1.2 Organization reliability

Insta's governance model has been implemented in such a way that responsibility, legal compliance, non-discrimination and customer commitments are at the core of operations. Insta has over 60 years of history with excellent financial history. Insta has liability insurance compliant to Finnish and European regulation.

### 4.1.3 Segregation of duties

Insta has defined and documented Trusted Roles and their responsibilities and the segregation of duties across these roles. Trusted Roles and segregation of duties is verified, maintained and reviewed regularly, at least annually.

## 4.2 Human resources

Insta has employed enough personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide Trust Services.

Verification of the background of all employees is done as part of Insta's HR policy. After termination of employment, the employee's confidentiality obligation remains in effect.

All roles and responsibilities are defined, including Trusted Roles, users named and documented. Named users have formal education and training and actual experience for their duties.

Operative Service Manager, responsible of ISMS, reports to top management of Business Unit.

In case personnel violate Insta's policies and procedures, disciplinary sanctions are defined according to The Information and Cybersecurity Policy.

## 4.3 Asset management

### 4.3.1 General

Insta maintains up-to-date inventories of its ICT assets, including Trust Service Systems.


Copyright © 2026 Insta Advance Oy

Trust Service System recovery plans are defined, and availability requirements of assets are aligned with the delivery and recovery objectives of those plans.

Asset management covers the entire life cycle of the assets, including acquisition, use, storage, transportation and disposal.

### 4.3.2 Assets classification

Insta's data classification guidelines are applied in the classification of Trust Service System. Insta conduct periodic reviews of the assets, including classification, and update them, where appropriate.

### 4.3.3 Asset handling and storage media

Insta has defined rules for the acceptable use of assets. Those rules include personnel and contractors' physical and electronic assets return to Insta.

Media containing sensitive data is securely handled and disposed of when no longer required. This includes a thorough erasure process or a secure disposal for physical media containing sensitive data.

Process is described in document Insta's methods and processes for destroying confidential material.

## 4.4 Access control

### 4.4.1 General

Access Control Policy is defined according to The Information and Cybersecurity Policy of Insta. This ensures that system access is limited to authorized personnel.

### 4.4.2 Privileged and system administration accounts

Privileged and system administration accounts are granted only to those users, who must have strong access level due to that role. Roles are documented, access rights are reviewed and usage monitored.

### 4.4.3 Administration systems

Administration systems are used only for system administration purposes. Such systems are separated logically from application software, which is not used for system administrative purposes. Administration system access is protected to through authentication and encryption methods.

### 4.4.4 Identification

Users have unique identity for network and information systems. Identities are reviewed and logging implemented.


Copyright © 2026 Insta Advance Oy

### 4.4.5 Authentication

Strong authentication is established for privileged accounts and system administration accounts.

### 4.4.6 Multi-factor authentication

Multi-factor authentication method is established for privileged accounts and system administration accounts.

## 4.5 Cryptographic controls

Insta has established appropriate security controls to manage cryptographic keys. All cryptographic keys are being used in relation to the services. Insta monitors that the used algorithms and key sizes are aligned with the regulation.

## 4.6 Physical and environmental security

Insta's premises have been built in accordance with Finnish national security criteria (Katakri). Insta Advance has been granted a Facility Security Clearance (FSC) certificate, which is updated regularly.

## 4.7 Operation security

Following processes and procedures are used as operational procedures:

- Change management
- Vulnerability management
- Secure development processes
- Secure testing procedures
- Acquisition procedures, part of Supply Chain management
- Malware control procedures

Processes and procedures are up to date and reviewed at least annually.

## 4.8 Network security

Vulnerability management procedures ensure that systems are up to date and reviewed.

Penetration testing is performed at least annually. Security scanning is done at least quarterly, typically weekly.

Zoning and filtering rules of the network are implemented in accordance with the principles of least privilege and defense in depth.

Network security controls include e.g. malware control procedures, protection against DDoS and secure connections between parties.


Copyright © 2026 Insta Advance Oy

## 4.9 Vulnerabilities and Incident management

### 4.9.1 Monitoring and logging

Insta's System Support personnel provide 24/7 continuous monitoring of the infrastructure, network and security components as part of their service offering.

Insta's Security Operations Center (SOC) maintains a situational awareness of the threat landscape, by monitoring events, with the aim of preventing or minimizing the impact of cybersecurity incidents. Based on specific rules, alerts are triggered for personnel to investigate possible suspicious events.

Monitoring system includes all components of ICT-environment, e.g. infrastructure, network components, software application processes.

Events and security transactions are logged, protection of logs is in use, clock synchronization is in use.

### 4.9.2 Incident response

Incident management includes handling policies and guidance, the roles, responsibilities and procedures for detecting, analyses, responding to, recovering, documenting and reporting of incidents in a timely manner.

### 4.9.3 Reporting

Security incident reporting covers notifications to supervisory authorities and CSIRTs, stakeholders, and other authorities in accordance with EU-legislation and its national implementation guidelines, e.g. GDPR, NIS2, DORA, CRA.

### 4.9.4 Event assessment and classification

Incident and event management include:

- Analysis of monitored or reported events
- Assessment of event severity and classification
- Suspicious events assessment to determine whether they constitute incidents
- Determining nature and severity of security incidents

### 4.9.5 Post-incident reviews

Insta prepares a Root Cause Analysis (RCA) report to customers in case of data security or privacy incidents, or in case of degraded Service Level. RCA-report is used for internal development and improvement.

## 4.10 Collection of evidence

Insta collects and maintains records concerning the operation of the services with the purpose of proving evidence of the correct operation of services. These records will only be disclosed to law enforcement authorities under authorities' order and to users with right to access them upon legitimate request.


Copyright © 2026 Insta Advance Oy

These records are protected and backed up to avoid information loss or compromise. Audit data log records are retained according to regulation.

## 4.11 Business continuity management

### 4.11.1 General

Availability management, Continuity management and Preparedness procedures are part of the Insta's ISO/IEC 27001 2022 certified ISMS. This ensures that process and procedures are in operation, disaster recovery plans exist and are reviewed. Preparedness procedures included redundancy of network and information systems, communication channels, personnel and other critical assets.

### 4.11.2 Backup

Backup plans and systems are in operation, RTO and RPO defined, backups are tested automatically and manually, backup copies are stored in safe locations and appropriate physical and logical controls are in use.

### 4.11.3 Crisis management

Major Incident Management procedures ensure that process and procedures are in operation, disaster recovery plans exist and are tested and trained with personnel and reviewed. Insta's senior management participates in major incident and crisis training.

## 4.12 TSP termination and termination plans

Insta has service termination plan that deals with termination notification, subcontractors management, information maintenance, private key destruction, termination phasing and updating of the termination plan procedure.

Insta has taken measures to ensure that funds will be available for the execution of the termination plan, also in case of bankruptcy.

## 4.13 Compliance

Insta Cyber Security Unit Executive Steering Group monitors evolution of legislation to make sure that the services are created and maintained aligned with any applicable legal requirements.

Insta employs personnel with the required skills and has fulfilled the required roles. Personnel supervise, according to their own role, fulfillment of required implementation of legal requirements.

Insta's processes and procedures are ISO/IEC 27001 2022 certified. Processes and procedures are annually reviewed by accredited auditor. Insta has obtained the Qualified status for its management of remote Qualified Seal Creation Device and is in this regard under supervision of the Traficom (Finland national supervisory body) and undergoes regular audits on this subject.


Copyright © 2026 Insta Advance Oy

## 4.14 Supply chain

### 4.14.1 Supply chain policy

Insta has The Supply chain policy which governs the relations with direct suppliers and service providers. Policy defines criteria for selecting and contracting suppliers. Policy defines principles of information security management of supply chain. Policy defines monitoring, follow-ups and changes of supply chain, too.

Supply chain procedures are reviewed at least annually.

### 4.14.2 Responsibility, third party agreements and SLA

Agreements are signed with service providers, defining the responsibilities and obligations of the parties. The parties review agreements contents regularly.


Copyright © 2026 Insta Advance Oy

# 5 SSAS Practice Statement

## 5.1 Policy claims

This practice statement is aligned with EU SSAS Policy [itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4)].

## 5.2 Publication and repository responsibilities

The Insta Trust Service Practice Statement is made publicly available via Insta's website: https://www.insta.fi/en/cybersecurity/services/qtsp/.

The information identified in Trust Service Practice Statement is available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall make best effort to ensure that this information service is not unavailable for longer 72 hours.

## 5.3 Signing key initialization

### 5.3.1 Signing key generation

Signing keys are generated within a secure Hardware Security Module (HSM), acting as a Qualified electronic Seal Creation Device (QSCD). The QSCD is certified according to Certification Report NSCIB-CC-2300116-01-CR version 1. The hardware is certified to EAL 4+, ensuring a high level of protection against both physical and logical attacks.

The cryptographic algorithms and key lengths employed have been selected to comply with current security standards and are ensured to remain sufficiently robust throughout the entire validity period of the certificate. The supported algorithms and key lengths are:

- RSA-4096
- ECC P-384

Device initialization is performed based on the four-eyes principle (dual control), requiring the participation of at least two authorized operators.

The key generation process is orchestrated by a separate Registration Authority (RA) application. The RA application triggers the key generation within the QSCD, ensuring that the cryptographic process occurs entirely within the device's secure environment. Following key generation, the RA application generates a Certificate Signing Request (CSR). This ensures that the private key never leaves the QSCD in plaintext and that neither the RA application nor any other external system can access the key.

### 5.3.2 eID means or identity linking

For the electronic seal creation service, the identity proofing and verification of the legal person is performed by the Digital and Population Data Services Agency (DVV). Upon


Copyright © 2026 Insta Advance Oy

successful verification and approval, the organization is issued a unique authentication certificate.

The linking between the verified identity and the sealing keys is established by mapping this authentication certificate to the authorized sealing keys within an authorization service. To initiate a sealing request, the requester must authenticate against this authorization service using the authentication certificate. The authorization service then verifies the identity and grants access to the corresponding sealing keys.

The integrity of this mapping and the authorization process is protected through a combination of technical and administrative controls:

Technical Protection: The authorization data and the links between certificates and keys are stored and managed in a secure environment, ensuring that unauthorized modifications are prevented.

Administrative Control: Unauthorized modification of the authorization server configuration is prevented by enforcing authenticated and role-based administrative access, restricting changes to secured management interfaces, and ensuring all configuration changes are logged and auditable.

### 5.3.3 Certificate linking

The SSAS is compliant with the requirements of EN 419241-1 for certificate linking. It implements the mandatory linking of signing keys to public key certificates, ensures that keys are not used before linking, and provides robust integrity protection for these links.

### 5.3.4 eID means provision

Described in paragraph 5.3.2.

## 5.4 Signing key life-cycle operations

### 5.4.1 Signature activation

Signature activation processes are implemented in accordance with EN 419 241-1. The system ensures that signing keys are activated and used under the authorized control of the relevant signing entity and only for signature operations explicitly authorized through the signature activation process.

Prior to any action that may impact the control or use of a signing key, the requesting entity is successfully authenticated. Secure protocols are used to protect signature activation against man-in-the-middle attacks, replay attacks, credential misuse, and other forms of impersonation. Access controls prevent any entity from accessing sensitive system objects or functions that could enable control over another signer’s signing keys.

Signing keys are activated only upon successful authentication and the presence of valid signature activation data (SAD). Activated signing keys are restricted to signing only the data to be signed (DTBS/R). The validity of the corresponding public key certificate is verified prior to use. Cryptographic algorithms and parameters are selected in accordance with applicable standards and recommendations to ensure resistance for the entire lifetime of the certificate. The allowed signature algorithms are:


Copyright © 2026 Insta Advance Oy

- RSA-4096 with SHA-384
- RSA-4096 with SHA-512
- ESCDSA P-384 with SHA-384

#### 5.4.1.1 Sealing (System-Based Authentication)

For sealing use cases, signature activation is based on authentication of an authorized client system acting on behalf of a legal person. Authentication is performed using customer-specific interface certificates and secure system-to-system communication mechanisms.

In these use cases, authentication is not linked directly to the identity of a natural person. Authorization and accountability are established at the organizational and system level. No individual identity verification process or individual signature session is required. All general signature activation controls described above apply.

### 5.4.2 Signing key deletion

Signing keys are securely destroyed when they are no longer required. All signing operations are performed within certified HSM devices, and signing keys never leave the HSM security boundary in plaintext form. Any references to signing keys stored outside the HSM are encrypted, with encryption keys protected by the HSM security context.

A signing key is destroyed when the corresponding public key certificate has expired or has been revoked, when the signing key is no longer required for its intended purpose, or upon a justified request from the signer or the customer organization. Where technically feasible, signing key destruction also covers all backups of the signing key to ensure that no residual information can be used to reconstruct the key.

#### 5.4.2.1 Sealing

For sealing use cases, signing keys are typically long-term, statically assigned to a customer organization and protected within the HSM. These keys are subject to regular key lifecycle management, including controlled key rotation. Sealing key securely destroyed when the associated certificate expires or is revoked, upon customer request, or upon termination of the contractual relationship. Sealing key destruction may also be initiated by the Trust Service Provider as part of operational key management procedures, such as decommissioning of services or cryptographic renewal.

### 5.4.3 Signing key backup and recovery

The Trust Service Provider ensures that all sealing keys are securely backed up and recoverable in a manner that preserves confidentiality, integrity, and controlled use. All sealing operations are performed exclusively within certified HSM devices. Signing keys are generated and remain within the HSM security boundary at all times and are never exposed in plaintext form.

When not actively used for cryptographic operations, sealing keys are stored outside the HSM only in encrypted form. Encrypted key material is maintained in a database, which is subject to regular system backups. Database backups and database dumps may therefore contain encrypted signing key material; however, such backups alone do not enable the use, activation, or reconstruction of any signing key. Decryption and


Copyright © 2026 Insta Advance Oy

operational use of signing keys is only possible within the HSM after restoration of the corresponding HSM security context.

Recovery of signing keys requires restoration of the HSM security context containing the Key Encryption Keys (KEKs) used to protect signing and sealing keys. Restoration of this security context is performed exclusively within the HSM and requires quorum-based authorization using administration smart cards held by different authorized operators. Quorum credentials are distributed in a manner that prevents any single individual from performing recovery operations alone.

All backup, storage, and recovery operations related to sealing keys, including HSM security context restoration, are performed only by explicitly authorized personnel and under controlled procedures. Where backups of encrypted signing key material exist, protection mechanisms ensure a level of security equivalent to or higher than that provided by the HSM itself. This approach ensures that signing keys can be securely recovered if required, while preventing unauthorized access or misuse at any stage of the backup and recovery process.

## 5.5 Additional facility, management, and operational controls

### 5.5.1 Audit logging procedures

Described in paragraphs 4.10 and 4.7.2.

### 5.5.2 Records archival

Described in paragraph 4.10.

### 5.5.3 Compromise and disaster recovery

Described in paragraphs 4.9 and 4.11.

### 5.5.4 SSASP service termination

Described in paragraph 4.12.


Copyright © 2026 Insta Advance Oy