IN GROUPE DENMARK PS

TSP PS

Document information			
No. of pages : 19	Reference : N/A	Department : eID Application Development	Classification : Public
Creation date : 17/02/2025		Last saved update: February 25	Version : 1.0

Version history			
Version	**Date**	**Author**	**Description of update Updated paragraphs**
1.0	17/02/2025 00:00	PEDERSEN, Sanne	Initial version
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		

CONTENTS

1 INTRODUCTION

IN Groupe provides a Qualified Signing Service that comprise of coordinating several Qualified Trusted Services, as defined under European Regulation [eIDAS], into one commercial signing service.

2 SCOPE

This is the general Practice Statement for the IN Groupe Denmark Qualified Trust Services.

It covers the general requirements as stated in [EN 319 401] and should be read as the operational and organisational foundation for the specialized practice statements for the Trust Services providing a Qualified Signing Service for our customers.

The structure for our practice statements:

- Trust Service Provider Practice Statement (TSP PS)
  - Certificate Practice Statement (CPS)
  - Remote Qualified Signature Creation Device Practice Statement (rQSCD PS)
  - Time-Stamping Authority Practise Statement (TSA PS)

We refer to the individual Practise Statements for references to standards covering that service.

3 DEFINITION OF TERMS, SYMBOLS, ABBREVIATIONS AND NOTATIONS

Term	Definition
CPS	Certificate Practice Statement
CMDB	Configuration Management Data Base
eIDAS	electronic Identification, Authentication, and Trust Services
HSM	Hardware Security Module
ISMS	Information Security Management System
ITSM	IT Service Management system
OWASP	Open Worldwide Application Security Projec
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
rQSCD PS	Remote Qualified Signature Creation Device Practice Statement
S-SDLC	Secure Development Life Cycle
TSA PS	Time-Stamping Authority Practise Statement
TSP PS	Trust Service Provider Practice Statement (this document)

4 CONTACT

The QTSP can be contacted using the following email address:

info@pki.ingroupe.dk

5 RISK ASSESSMENT

The Risk Management is integrated in the Information Security Management System.

Risk Management is supported by a Secure Development Life Cycle (S-SDLC) framework that ensure that development and maintenance of the applications consider the current threat landscape and determine our response from initial Security by Design all the way to actual code reviews.

The Risk Assessment for the QTSP is based on the defined assets of the solution. Risk scenarios for each asset are identified and evaluated against the implemented controls resulting in a risk score.

This procedure allows us to not only identify risks but also evaluate if the control measures provide mitigation to provide an overall acceptable residual risk.

The Risk Assessment is reviewed yearly or if one or more of the following actions occur:

- Changes in the known threat landscape.
- Updates in the trusted services that cause addition or removal of assets.
- Major updates in the trusted services causing major changes in the use of assets.
- Updates that cause addition or removal of mitigating factors

Revisions of the Risk Procedures and Assessment are approved for TSP Management.

6 POLICIES AND PRACTICES

6.1 Trust Service Practice Statement

The policies and practice statements are declared in the practice statements for the relevant services [CPS, rQSCD PS, and TSA PS]. For the respective policies, all requirements are met.

The QTSP uses services from external organizations for the provision of the services and has agreed obligations, policies, and procedures.

The practice statements [CPS, rQSCD PS and TSA PS] are publicly available 24/7 at the website https://pki.ingroupe.dk/repository/. Due notice of revisions is provided for affected subscribers and relying parties at the repository. New practice statement versions are published well in advance of date they have effect.

The practice statements are reviewed at a regular basis. The following events can trigger a revision of the practice statements:

- Changes in relevant regulation, i.e. a new or amended eIDAS implementing act.
- Changes in relevant standards.
- Requirements imposed by the Supervisory Body.
- Development in business requirements.

The TSP Management approve revisions prior to publishing new versions of the practice statements and notify the Supervisory Body of corresponding changes.

6.2 Terms and Conditions

The following terms and conditions for the QTSP services are publicly available for download on https://pki.ingroupe.dk/repository/.

End-user terms are also made available directly via link when signing allowing the user to be informed before proceeding to use the service.

Liabilities and limitations are described in the Terms.

6.3 Information Security Policy

As part of our Information Security Management System (ISMS) the QTSP has implemented an Information Security Policy to govern the implementation of secure operations through development, maintenance, and

operation of our services. The Information Security Policy is internally available and communicated to all employees impacted by it.

The Policy reviewed regularly and further evaluated on the same basis as our Practice Statements when a potential triggering event occur.

The Policy and its subsequent updates are approved by TSP management prior to implementation. If changes to the Policy have consequences to subscribers or relying parties, this will be reflected and communicated in corresponding updates of the relevant Practice Statements and/or the related Terms and Conditions.

The Policy introduce guidelines on secure practices in handling access, IT, and physical interactions to provide all employees with a clear picture of common security threats in their daily work.

The Information Security Policy is also the foundation for our threat modelling and subsequent Risk Assessment.

The Policy govern yearly checks of our inventory of assets and their configuration.

7 TSP MANAGEMENT AND OPERATION

7.1 Internal Organization

7.1.1 Organization Reliability

The QTSP is founded and owned by IN Groupe, a renowned, international business providing the financial stability and insurance to operate the services and ensuring our financial liability.

The QTSPs services are available to subscribers and relying parties within our field of operations under the Terms for the services.

To comply with [eIDAS] Article 24 section 2c, the QTSP has an insurance which complies with the national legal requirements in Denmark, the country where the QTSP is established and supervised.

The QTSP can be contacted through https://pki.ingroupe.dk/repository/ for business enquiries, GDPR requests, questions, and complaints.

Complaints will be handled through our internal process, starting with confirming by e-mail to the plaintiff, that the issue has been received and describing next step in the process.

SP management, senior staff and personal in trusted roles have declared they are free from any commercial, financial and other pressures which might adversely influence trust in the services it provides. The QTSP is organised to ensure impartiality of operations.

7.1.2 Segregation of Duties

Duties and responsibilities are segregated through organisation, roles, and access control to reduce the risk of misuse of the QTSP assets.

7.2 Human Resources

To ensure qualified personnel throughout all levels in the QTSP, hiring is based on requirements for experience, training and credentials for the future employees' function and role. The individual qualifications must cover the basic job requirements while the QTSP, upon hiring, supplement with specific knowledge on policies and procedure guiding daily conduct.

Generally:

- Mandatory yearly updates on the Security Policy reflecting the current threat landscape for the services.
- Additional security education relevant to the specific profile, e.g. security by design, secure coding, top 20 OWASP threats etc.
- Ways of working including policies for working securely inside and outside of the office

Specifically for trusted personnel:

- Timely, certified and qualified product specific training

Contractors must apply their own corresponding Information Security Policies to be in accordance ours.

All access to the QTSP services is based on segregation of systems and functions, and under general access control. Rights to access are provided by management under a profile for the function. Further access can be granted on an individual basis for instance to personnel with specific Trusted Roles.

Trusted Roles are defined in the Security Policy by a Security Officer. The roles are assigned the personnel trained in and working directly with the specific secure elements of the services.

Trusted roles are not assigned as a part of a general job profile, but on a strict need-to-use basis, limiting the trusted personnel to trained employees performing specific tasks related to the secure elements.

Trusted roles are assigned by management and accepted by the employee.

7.3 Asset Management

7.3.1 General Requirements

The assets of the QTSP, including information assets, are protected throughout the supply chain for the services.

7.3.2 Assets Inventory and Classification

Physical and logical assets are registered in a Configuration Management Database (CMDB) providing documentation for both the inventory, the classification and the relationships between elements.

The asset list is closely related to the change management system and impacted assets are reviewed, when impacted by changes.

The QTSP provides high-availability services and the related Service Levels for availability, and Disaster Recovery plan for data restoration and recovery, reflect this.

The full asset list including information the asset list is reviewed in conjunction with the recurring Risk Assessment.

The procedures for implementing, operating and terminating assets are anchored in the Information Security Policy to ensure control of the assets in their entire life cycle.

7.3.3 Storage Media Handling

The general policy for storage media in the QTSP Security Policy precludes the use of unauthorized storage media on any device on the QTSPs network from employee PCs and upwards. In daily use access-controlled file sharing or storage via online repositories is encouraged as a more secure alternative.

When necessary for specialized actions the storage media used must be approved and provided by the QTSP. Storage media are kept secured from initialisation to disposal. Storage of media in use is differentiated from reflecting the confidentiality of the data and its function in the solution.

Data being stored for a significant period of time is kept in media regularly controlled against data deterioration.

7.4 Access Control

The QTSP systems are under access control supplemented with a series of access rights allowing restricted access according to job profile and individual privileged roles under the principle of “least privileges”.

All employees will have access to general IT-functions such as e-mail, time registration etc.

Employees in a job function will further be given general access rights to functions specific for their daily work.

Personnel with specific or senior responsibilities and completed training in secure data handling will further be given access to the systems they operate. Access rights on this level are system or function specific.

Trusted roles and their corresponding access rights are only assigned to individuals after verification of their reliability and training in the specific systems they operate. The training includes handling the data stored in

secure areas from the time of storage to their secure disposal. Access to the secure areas is – in addition – under dual control and access to systems in that area require 2-factor login.

The assignment of trusted roles is monitored by the Security Officer as part of the ISMS.

All assigned roles are reviewed yearly by management to maintain the “least privileges” principle and to reflect an employees’ responsibilities or training. All access rights are terminated with ended employment.

7.5 Cryptographic Controls

Cryptographic keys, algorithms and devices are managed through their lifecycle through monitoring and controls.

The QTSP inspects new cryptographic modules not to have been tampered with before they are installed within the QTPS environment. The QTSP environment is physically protected and only authorized personal in trusted roles are allowed to access the environment for specific purposes. In addition, to the protection made by the secure environment, the QTSP inspects the cryptographic modules at regular intervals.

All actions carried out by QTSP personal involving cryptographic modules requires at least dual control.

For secure elements and audit log the associated HSMs handles the key lifecycle.

The QTSP uses cryptographic modules which meets the requirement [EN 419 221-5], which is a protection profile with product evaluation of EAL4. Private keys related to root CA, CRL issuing, issuing CA, OCSP responder, time-stamp issuance and subject private keys are generated, protected and used within these modules. The keys are always protected by the cryptographic module. The keys are not backed up

Private keys residing in a cryptographic module are deleted before the module is decommissioned.

For service-to-service communication the platforms certificate manager function performs a corresponding role.

7.6 Physical and Environmental Security

All premises, where work pertaining the QTSP is done, are protected with physical access control.

The QTSP systems are operated in data centres with a protected security perimeter providing protection e.g. in the form of physical access control, video surveillance and patrols. The core elements, as defined through the risk assessment of the solution, are further protected in secure areas under logged dual access control.

Two employees with a relevant Trusted Role may access the secure room and together ensure that controls to prevent loss, damage or compromise of assets do not occur are maintained though following secure room processes. Similar processes also prevent compromise or theft of information and equipment.

7.7 Operation Security

To provide a service with built in IT-security QTSP choose systems and products based on their functionality and the technical security and reliability they support.

During operations the systems integrity are protected through regular vulnerability scans to identify both malicious and unauthorized software and vulnerabilities identified in system elements and acting on the findings.

Service stability and security in operations is provided via change management procedures for all modifications of hardware, software and configurations. To further support chance management, the process is system coordinated and documented.

Changes are performed following procedures for the trusted and administrative roles that work with the service.

Security patches for the systems and products in the service are evaluated when they are released. If they do not introduce other vulnerabilities or instability that outweigh their benefit they are implemented within a reasonable time. The result of the evaluation is documented if the patch is not applied.

The systems and products of service is registered in a configuration management database that support the monitoring and review of the configurations of hardware, software, services and networks.

The QTPS monitors the use of its system to project changes in capacity demands.

7.8 Network Security

The network is designed based on a risk assessment of the assets and reflecting the impact of an attack or loss of data by establishing the operational network as separate and segmenting the elements of the solution into 3 different zones from DMZ over Application zone to Secure zone. The rules are revisited with the yearly update of the Risk Assessment.

The edge of the solution is protected by firewalls restricted to whitelist and allowed protocols access.

The DMZ hosts endpoints for services and applications for presenting the services online at the customer.

The Application zone contain the core services and PKI components infrastructure components used in the Qualified Signing Service.

The Secure Zone contain the Hardware Security Modules (HSM) and the Qualified Signature Creation Device (QSCD) and function as repository for the Root CA.

Communication between zones is controlled by encrypted connections that restrict access defined as network policies between specified elements and only in one direction; the DMZ zone can only initiate connections to Application zone services, while the Application zone can only initiate connections to Secure zone components. Direct communication between the DMZ and Secure zones is not permitted.

The network infrastructure is mirrored across datacentres with failover functionality allowing a redundant high availability setup.

This design structure is also repeated in test environments allowing development and internal Quality Assurance with a high degree of fidelity. One test environment is available for customers integrating to the service.

The network undergoes daily, automated vulnerability scans with a system generating reporting in the form of notifications for evaluation and processing.

The automated scans are supplemented by penetration tests performed when required by a significant update of the system, or at least once a year. Penetration tests are performed by an external party and result in a report detailing the findings. Findings from penetration tests are evaluated and processed like the findings from the vulnerability scans.

The QTSP provide personal computers equipped with malware detection and removal software, that is updated at least daily, when the computer has access to mail and internet and connected to the network.

The QTSP hardens its equipment for operation of the QTSP services such that only accounts, applications, services, protocols and ports used by the QTSP services are enabled.

7.9 Vulnerabilities and Incident management

7.9.1 Monitoring and logging

Monitoring is established on endpoints and metric exposure validation. The logged information is processed by the monitoring system triggering alerts with levels according to pre-configured thresholds according to number of events and service criticality. The generated alert level determines the relevant response from ‘information only’ to raising a high-level incident requiring immediate resolution.

All monitoring logs are retained for 30 days. Audit logs are retained for seven years.

The QTSP and the platform provider maintain logs on all relevant activities in the system.

7.9.2 Incident response

The incident response procedures for the QTSP and the platform provider define processes for containment, eradication and recovery to minimize damage from security incidents or malfunctions.

The process includes categorisation of incidents and response plans according to category including communication and subsequent reporting. Incident management is coordinated through a command bridge function with the knowledge, training and authority to include the resources necessary to respond to an incident. This includes involving and informing key management in decision making to ensure business continuity when necessary for crisis management.

The incident procedures include communication plans between internal stakeholders. External stakeholders are informed according to their agreed communication plans.

All actions and findings during an incident are documented in the IT service management (ITSM) system preserving the data to make the follow-up concise.

Follow-up on incidents includes root cause, response and solution analysis determining if the incident will trigger updates in systems, configuration, or procedures to mitigate or eliminate recurrences. The follow-up results in a plan for mitigation or reasoning as to why no steps to remediation are taken. For critical vulnerabilities a remediation is carried out within 48 hours. For other vulnerabilities the QTSP either drafts and executes on a plan for mitigation or documents the reason for the vulnerability not to require a remediation.

If an incident is identified as an information security incident the follow-up is appointed to trusted role personnel allowing the QTSP to report to the supervisory body as defined in [eIDAS].

7.9.3 Reporting

The QTSP notify the appropriate parties on https://pki.ingroupe.dk or directly, in line with the applicable regulatory rules, of any breaches of security or loss of integrity that has significant impact on the trust services or the personal data therein within 24 hours of being identified.

Where a natural or legal person, to whom the trusted service has been provided, is involved, that person is also notified without delay allowing current contact information is available.

The QTSP allows staff, contractors and customers to report possible incidents using the contact information supplied in section 4.

7.9.4 Event assessment and classification

During incident handling the events are continually analysed and evaluated based on the accumulated knowledge and data.

Consequently, the severity of the incident can be raised or lowered with a corresponding updated plan of actions.

7.9.5 Post-incident reviews

Independent of the incident process the system is under automatic vulnerability scans and the resulting findings are addressed to reduce the risk of vulnerability-based incidents.

Post incident reviews involve resources with knowledge of the technical vulnerabilities of the elements in the system. The review shall identify the root cause of the incident and possible measures to mitigate recurrence of similar incidents.

For each incident a post-incident is performed. The scope of the review will span from simple evaluation to creating a problem task force depending on incident categorisation and event complexity.

7.10 Collection of evidence

The QTSP generates audit record for all events related to security, CA services and TSA service. Whenever there are automatic systems in place the logs are collected to the same storage. Other logs may be used whenever this is not possible.

Logs related to security are kept and may be made available for the QTPS conformity assessment body.

The logs include information on:

- Start and shutdown of the audit log,
- System start and shutdown,
- Security policy,
- System crashes and hardware failures,
- Firewall and router activities
- Issuance of certificates
- Events related to CA, TSA and subject keys.

The QTSP persist audit records in its systems. The records are protected in integrity and confidentiality. Each record includes the time, synchronized with UTC, of the record event. The events do not contain system sensitive information.

Relevant parts of the audit logs are checked at regular basis for any inconsistencies.

Access to the audit logs is authorized to personnel, who may read the records. Deletion of audit records may be carried out once the relevant entries has been exported to an archive.

At scheduled intervals, the audit records are exported for external storage. The integrity and confidentiality protection are inherited in the archive.

The QTSP maintains audit information for at least 7 Years.

7.11 Business continuity management

7.11.1 General

The QTSP maintains a disaster recovery plan describing multiple threat-based scenarios including the compromise of a private signing key or other credentials of the TSP.

The plan includes immediate steps to recovery and subsequent remediation of the system for each scenario.

7.11.2 Back up

The system and its supporting databases are replicated across data centres providing live failover to provide fast recovery and minimal data loss. Restore from back up is tested at regular intervals.

In addition, archiving of audit logs is implemented through periodic database dumps stored on external storage media. Each archive operation generates a timestamped dump of the audit log records from the relational database. The dumps inherit the existing encryption and integrity protection mechanisms of the live audit log system. Further upon creating each timestamped dump a SHA256 hash is generated on the dump for easier integrity checking. Archived dumps are included in the regular database backup routine, providing redundancy through backup copies maintained on separate storage media.

This implementation ensures compliant long-term preservation of the audit logs while maintaining the evidential value for digital signatures.

7.11.3 Crisis management

The QTSP have established processes for crisis management addressing

- Roles and responsibilities in crisis situations
- Communication plan between the QTSP, relevant competent authorities and customers
- Appropriate controls for maintain information and network security

The QTSP evaluate information from the Danish CSIRT and other competent authorities to determine if the information should trigger updates of the crisis management plan.

If the QTSP identifies issues with processes during the incident review process, including the crisis management plan, the processes will be updated.

7.12 TSP termination and termination plans

The QTSP has a termination plan for the termination of the trust services.

Prior termination of one or more services, general notification will be provided at the QTSPs repository.

In addition, the supervisory body, relying parties and other parties with whom the QTSP has established a relation will be informed.

All authorizations for sub-contractor and third parties to act on behalf of part of the affected services, will be terminated. For instance, identity verification providers and identity providers will no longer be able to provide verified identities as part of certificate issuance.

The QTSP will maintain records as evidence for legal proceedings.

Key material for the provision of the affected services will be destroyed and the service discontinued. In case a certification service or time stamp service are terminated, the impacted certificates will be revoked.

Revocation status information of CA and TSA certificates will be made available in a CRL available at the QTSPs repository to ensure impact on subscribers and relying parties are minimized.

The QTSP does not hand over personal date as part of termination.

7.13 Compliance

The QTSP is conformity assessed to meet the requirements in the [eIDAS] regulation providing the legal framework for qualified trust services. The result of the assessment is provided for the Danish supervisory body for approval and granting the QTSP of its qualified status.

The QTSP is assessed with a regular frequency as stipulated in the [eIDAS] regulation.

The end user products provided are tested for accessibility according to WCAG 2.1 as outlined in [EN 301 549] and made available for people with disabilities where feasible.

Measures are implemented against both unauthorized or unlawful processing of personal data through technical design protecting the data and organization restricting access to data on the “least privilege” principle. Similarly, data is protected against accidental loss or destruction through redundant data systems, integrity testing of data and backup on separate storage media. Processing of personal data is described in the Terms and Conditions for the services and in the data processing process, both available in the QTSP repository.

7.14 Supply chain

7.14.1 Supply chain policy

The QTSA has implemented an ICT supply chain policy and procedures for assessing suppliers, services and products and identifying security risks. Vendors are evaluated against:

- Price and value
- Quality assurance
- Reliability
- Financial stability
- Compliance and
- Sustainability

Agreements with suppliers and customers define the QTSP’s role in the supply chain and associated risks for acquired assets are included in the risk assessment for the trusted services to provide a coordinated risk assessment.

7.14.2 Supply chain procedures and processes

The ICT supply chain policy outline risk assessment of ICT products and services including evaluation of the relevant security requirements for the delivery through its lifecycle.

Agreements with suppliers ensure that the security requirements are propagated onto their suppliers and sub-contractors. They include definitions for communication and data processing. TSP management review suppliers evaluating conformity, service delivery, dependencies, and alternate suppliers at least yearly.

Suppliers are required to provide information describing

- Software used in product
- Security functions of the product
- Configurations for the product's secure operation

The QTSP has processes for implementing products, verifying their integrity, testing their functionality and subsequently monitor that they conform to the stated security requirements.

Components for the trusted services are registered in a configuration management data base (CMDB) and categorised. Components are risk assessed and implemented in network zones according to criticality. The ICT components lifecycle is incorporated in general maintenance and patching processes.

The QTSP does not use cloud services providing the trusted service but may make use of cloud based services for other purposes not directly involved.

7.14.3 Responsibility, third parties' agreements and SLA

The QTSP will maintain overall responsibility for conformance when making use of suppliers to provide parts of its service through subcontracting, outsourcing or other third-party arrangements. These requirements will be governed through a contractual relationship defining the outsourcers liabilities and requiring their implementation of any controls required to document their compliance to the relevant information security requirements.

The supplier shall implement processes and procedures to support

- Those implemented by the TSP as specified by the policies and requirements included in the contract
- Those required to implement the supplier's services or products
- Those required to terminate the use of the supplier's services or products

When using a trust service provided by another party the QTSP ensures that the security and functionality meet its requirements. Likewise, when the QTSP makes use of interfaces to trust service components provided another party, it will ensure to meet the requirements of use as specified by said provider.

The contracts' service level agreements require auditing mechanisms that address the supplier's compliance with the QTSP information security requirements.

Compliance with information security requirements is a factor when TSP management review suppliers as defined by the supply chain policy. Evaluation of security incidents in supplier's services or related to the supplier's products is included in the regular review and can trigger an additional review depending on severity and impact.

The QTSP maintain a register of suppliers and agreement that allow review and tracking of

- Where QTSP information is stored and managed
- That the purpose of the agreement is adequate
- That the agreement is valid
- That the contract includes the necessary information security clauses

8 REFERENCES

References	
Text reference	**Description**
[eIDAS]	REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
[EN 319 401]	ETSI EN 319 401, Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers, v.3.1.1
[CPS]	https://pki.ingroupe.dk/repository/
[rQSCD PS]	https://pki.ingroupe.dk/repository/
[TSA PS]	https://pki.ingroupe.dk/repository/
[EN 301 549]	Accessibility requirements for ICT products and services v.3.2.1
[EN 419 221-5]	CEN EN 419 221-5, CEN TC224 WG17, Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, 2016.