PS for Remote Electronic Seal with Remote QSCD

Version history

Version	Valid from	Approved by (Title and name)	Comments
1.2	08.01.2026	COO / Christel Victoria Høst	Details about Penneo's qualified remote sealing service, incl. management of RQSCD as per ETSI TS 119 431-1, and EULA for signers. Document title updated to reflect this scope of service. General re-wording and alignment with standard terminology throughout the document for clarity and consistency. 1.6 updated accordingly. Added 4.9, 4.10, 4.11 and 4.12 regarding revocation, CRLs, status services, end of subscription, key escrow and recovery.
1.1	27.12.2024	Information Security Manager / Fredrik Lernevall	Improved readability.
1.0	22.11.2022	Information Security Manager / Fredrik Lernevall	First release

1. Introduction

This document supplements the Trust Service Practice Statement (TSPS). As a Practice Statement (hereinafter PS) it provides additional information and further specifies the procedures, activities and rules of specific services that Penneo implements in the management of Remote Qualified Seal Creation Device (RQSCD) and provision of qualified electronic signatures (hereinafter Service) based on the ETSI EN 119 431-1 standard.

Penneo's trust services are designed and operated to comply with Regulation (EU) No 910/2014 amended by Regulation (EU) 2024/1183 ("eIDAS") and other applicable EU regulation.

The service is provided to subscribers on the basis of the particular Certificate Policy for Qualified Remote Electronic Seal Certificate (hereinafter CP) which describes Penneo's certified Public Key Infrastructure and as defined by the RFC 3647 standard.

1.1. Overview

This PS describes the facts related to the life cycle processes of the certificate issuance and seal creation using a RQSCD and follows the structure of the standard RFC 3647, taking into account the applicable technical standards and principles.

The document contains only additional information to relevant chapters found in the TSPS, hence why not all nine chapters from the TSPS are included:

Chapter 1 - provides 1) information about this document with a unique identifier, 2) description of the entities involved in the preparation, organisation and administration of the operation, 3) description of the implementation of Penneo’s services and 4) defines the appropriate and prohibited use of certificates.

Chapter 3 - describes the process of identification and authentication for the creation of a certificate, respectively certificate revocation or suspension. Describes methods for proving possession of a user's private keys and the uniqueness of names.

Chapter 4 - describes the processes of the complete certificate lifecycle: the application for issuance, the process of issuing certificates, confirmation and approval of certificates, including notification of certificate issuance. The chapter also covers certificate revocation process, re-key and revocation lists.

Chapter 6 - describes the technical side of security of public and private key generation, cryptographic standards, algorithms used. Describes methods for activating and deactivating private keys. It addresses computer and network security, their principles and required control mechanisms.

1.2. Name and document identification

Name and Identification of the document:

Practice Statement for Remote Electronic Seal with Remote QSCD (RSA algorithm).

1.3 Trust services participants

1.3.1 Certification Authority for remote electronic signature and seal

Penneo is a Qualified Trust Service Provider under the eIDAS regulation:

- Issues certificates for remote and qualified electronic signature and seal
- Operates and manages trusted systems to support Penneo's electronic signature platform (hereinafter the Platform), based on applicable standards, including:
    - A web based Signer Interaction Component (SIC);
    - Remote Qualified Signature Creation Device (RQSCD);
    - Remote Qualified Seal Creation Device (RQSCD);
    - A Server Signing Application, to securely facilitate the connection with the RQSCD for the creation of Qualified Electronic Signature and Seal.
    - Other applications to support the Platform;
- Uses the services of third parties in a scope necessary in its activities, including cloud services, data centre and time synchronisation services.

Penneo also provides tools for customers to administrate their documents and requests for signatures to subscribers, including:

- A web application
- Public APIs

- Other integration tools

The use of these administrative tools has no implication on the provisioning of Penneo's qualified trust services.

1.3.2. Subscribers

The Subscribers are customers (legal persons) and signers (natural persons). Customers use the Platform to request signatures from other parties. Signers (including employees of companies, organisations or other legal entity) use the Platform to sign documents using their personal certificates for electronic signature. The Platform uses Penneo’s certificate for electronic seal to seal the documents upon completion of the signers’ signatures.

The Subscribers use the Platform services remotely through internet connection and web pages.

1.3.3. Relying parties

Relying parties are entities (natural or legal) that rely on and use Certificates issued by Penneo in their activities and that verify the remote electronic seal of signed documents based on the CA's hierarchy.

Information about Penneo's Trust Service including the Qualified Remote Electronic Seal Certificates is made publicly available via https://eutl.penneo.com

1.3.4. Other participants

Penneo relies on third-party suppliers to perform certain activities on a contractual basis:

- Data centre services,
- Hardware suppliers,
- Software suppliers,
- Cloud solution provider,
- Time synchronisation provider

The suppliers' obligations and liabilities are described in the bilateral contracts with Penneo. Relevant parts are mentioned in Penneo's internal documentation.

Penneo is fully responsible for the activities of the contracted suppliers. Risk assessments are performed. In the case of a breach, an investigation is conducted. Based on the results, the supplier may incur a penalty or termination.

Penneo secures stable operation but is not liable for irregularities in operations caused by factors that are outside Penneo's control. Penneo will restore normal operations as soon as possible according to internal Business continuity procedures.

Penneo ensures availability of the Platform during the term of the Agreement - uptime of 99.9%.

Other participating entities may be:

- supervisory authorities
- law enforcement authorities.

1.4. Service usage

1.4.1. Appropriate certificates uses

Certificates issued by Penneo under the Certificate Policy and Practice Statement may be used for qualified remote electronic sealing of documents in accordance with legal regulations.

1.4.2. Prohibited certificate uses.

Unauthorized use of a certificate means any use of the Certificate that is in conflict with the type of the Certificate and the CP under which it was issued or the appropriate use.

1.5. Policy administration

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 1.5 of Trust Service Practice Statement.

1.6. Definition and acronyms

Definitions

Penneo's CA Services	A set of certification authorities which is possible to use during electronic signature and electronic sealing - Root CA, subordinate CA, TimeStamp CA.
Penneo's PKI Services	Penneo's CA Services and qualified services for remote electronic signature and remote electronic sealing and stamping.
Certificate	A data message issued by a certification service provider combines data (code or public cryptographic keys that are used to verify an electronic signature) to verify signatures with the signer and allows to verify his/her identity.
Public Certificate Registry/Repository	An electronic registry where certificates and lists of revoked end-user certificates and service certificates are published. It is accessible according to the rules defined in the Certification Practice Statement or Certification Policy (CPS/CP) document.
Certificate policy (CP)	A set of rules that assess the applicability of certificates within individual groups and / or classes of applications in accordance with security requirements and is supported by Certification Practice Statement (CPS). It relates to the use of the certificate and to the use of data for the verification of the electronic signature of the holder for which the certificate has been issued.
Certificate Practice Statement (CPS)	It forms the framework of the rules set by the CP. They define in their procedures, provisions and regulations the requirements for all services entering the registration and certification process.
Certificate Revocation List /Repository(CRL)	List of expired certificates published by the Certification Authority to the Public Certificate Registry/repository (LDAP)

Electronic Signature	It expresses the general concept of signature, which is applied in an electronic environment. A wide range of means and technologies are used to generate this signature, including digital signatures and biometric methods.These are data in electronic form, which are attached to or logically connected to the data message and which enable the verification of the identity of the signer in relation to the data message.
Digital Signature	It is based on the use of cryptography (cryptosystems) with a public key. Currently, this term is used to refer to a special type of electronic signature. This type of electronic signature is used to verify the identity of the sender of the message or the person who signed the message. It is also used to verify that the message to which the digital signature was attached is not altered/modified.
Asymmetric cryptography - RSA	The principle of the method is that data encrypted by one of the keys can only be decrypted with knowledge of the other of the key pair and vice versa. One of the keys is called private, the other public. The RSA algorithm is used for asymmetric cryptography.
Private key	Data for creating a digital signature. Private part of an asymmetric key pair for cryptographic purposes. Used to sign and decrypt messages.
Public Key	Digital signature verification data. Public part of an asymmetric key pair for cryptographic purposes. Used to encrypt messages and verify digital signatures.
Registration Authority (RA)	Companies which are responsible for verifying the application for a certificate, identifying and authorizing the subscriber.
Electronic Seal	An electronic seal is a piece of data attached to an electronic document or other data, which ensures data origin and integrity.

Revoke the certificate	To terminate the certificate based on the responsible user's/manager’s request. The certificate cannot be renewed.
Suspension of the certificate	Suspend the certificate based on the responsible user's/manager’s request. Validity can be renewed.
Relying Party	An entity that relies on trust in a certificate and an electronic signature verified using that certificate.
Root CA	CA issuing certificates to Subordinate CA
OCSP responder	A server that provides public key status information in a certificate using OCSP protocol
Subordinate CA	CA issuing certificates to subscribers and relying services
TimeStamp CA	CA issuing certificates with time-stamp to subscribers

Acronyms

eIDAS	REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS 2 Regulation) provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.
PKI	Public Key Infrastructure - set of services (HW and SW) performing the all activities concerning to certificate life-cycle.
EJBCA	PrimeKey’s EJBCA is one of the longest running CA software projects, providing time-proven robustness and reliability. EJBCA is platform independent, and can easily be scaled out to match the needs of your PKI requirements, whether you're setting up a national eID, securing your industrial IOT platform or managing your own

	internal PKI. EJBCA covers all your needs - from certificate management, registration and enrolment to certificate validation.Software provided by PrimeKey. https://www.primekey.com/
LDAP	Lightweight Directory Access Protocol - Public Certificate Registry
OID	Object identifier (OID) - is an identifier mechanism used for naming objects based on a recognised standard by the International Telecommunication Union (ITU) and ISO/IEC that ensures globally unambiguous persistent names.
RA	Registration authority
IP	Identity providers
CA	certificate authority
TSA	Time stamp authority
UTC	Coordinated universal time
TSP	Trust service provider
HSM	Hardware security module
CRL	Certificate revocation list
CCID	Chip card interface device
DKEK	Device Key Encryption Key
UPS	Uninterruptible Power Supply
RQSCD	Remote Qualified Signature Creation Device Remote Qualified Seal Creation Device
SAM	Signature Activation Module
SAD	Signature Activation Data
SAP	Signature Activation Protocol
SIC	Signer Interaction Component
EULA	End User License Agreement

2. Publication and Repository Responsibilities

📌 This document does not bring any additional information to the Publication and repository responsibilities. For relevant information please see chapter 2 of Trust Service Practice Statement.

3. Identification and authentication

3.1. Naming

The naming scheme of Penneo's qualified trust services is approved by Penneo's managers and implemented by authorized Penneo employees.

3.1.1. Types of names

The structure of naming conventions is implemented in accordance with the scheme of the X.501 standard (resp. X.520 standard), valid standards and directives.

3.1.2. Need for names to be meaningful

All name information provided should be in accordance with internationally accepted standards and rules. Name structure is significant and is part of the certificate.

3.1.3. Anonymity or pseudonymity of subscribers

No anonymity or pseudonymity is supported.

3.1.4. Rules for interpreting various name forms

Naming conventions are implemented according to the rules of approved internal registration process and they exclude different interpretations.

3.1.5. Uniqueness of names

Unique names are created during the process of preparation and initialization of the certificate.

3.1.6. Recognition, authentication, and role of trademarks

Trademarks are defined by Penneo. Trademarks are verified during the registration process and added to the certificate structure.

Trademarks are verified in the registration process and added to the information in the certificate. Certificate subscribers are responsible for misuse.

3.2. Initial identity validation

Initial an identity verification and validation for certificates is performed through defined rules and procedures of Penneo and described in the internal documentation.

3.2.1. Method to prove possession of private key

The private and public key generation is performed with participation of Penneo's authorized employees and under controls of Penneo's management. The process follows a written procedure as defined internally and is recorded. The private key of the seal certificate is saved in the cryptographic hardware security module. Possession of the private key is not verified.

3.2.2. Authentication of organizational identity

Penneo only issues qualified electronic seal certificates to the Penneo A/S entity for Penneo's qualified electronic seal to be applied through the Platform's automated process. Penneo is the owner of the private key and the certificate.

Penneo’s PKI service is configured to ensure that the seal certificate can only be used to seal documents upon requests from the Platform. Automated requests for sealing of documents is implemented as part of the Platform’s process.

Penneo does not issue certificates for qualified electronic seal to other legal entities. Penneo's authorized employees confirm the seal certificate issuance with Penneo's management.

3.2.3. Authentication of individual identity

Penneo does not identify individual representatives of other legal entities for the purpose of seal certificate issuance.

Subscribers relying on Penneo’s seal certificate are customers (legal persons) and signers (natural persons). Customers use the Platform to request signatures from other parties. Signers (including employees of companies, organisations or other legal entities) use the Platform to sign documents using their personal certificates for electronic signature. The Platform uses Penneo’s certificate for electronic seal to seal the documents upon completion of the signers’ signatures.

Customers have an Agreement with Penneo and their subscribers are authenticated by subscriber’s unique ID identifier. Before signing, signers agree to the Signature Acceptance Note, thereby accepting Penneo's End User License Agreement, certificate documentation, policies and practice statements. All subscribers are assigned a unique subscriber ID identifier by Registration authorities.

The Platform does not allow subscribers to obtain and use a seal certificate for their own legal entity.

3.2.4. Non-verified subscriber information

Certificates are only issued to Penneo, for Penneo’s seal to be applied to customers' documents through the Platform’s automated process. Only Penneo's authorized employees have access to perform the certificate issuance, and they do so under control of Penneo's management. Certificates for electronic seals are not issued to other subscribers.

3.2.5. Validation of authority

Certificates of the subordinate CA for signature and seal are automatically implemented in the Platform's PKI services.

Validation of certification authority is fully automated process of the application developed by Penneo - The Platform and corresponding PKI services.

3.2.6. Criteria for interoperation

Penneo’s CAs and PKI structure is created to allow subscribers to create remote qualified electronic signatures. It also enables the addition of qualified timestamps as part of the signature creation, and addition of Penneo’s qualified electronic seal

to the signed documents. Penneo’s CAs and PKI do not implement connections with other CAs or other ways of interoperability.

3.3. Identification and authentication for re-key request

Penneo’s CA services do not support the act of re-key. Identification and authentication is performed based on Key Management processes and under Penneo management.

3.3.1. Identification and authentication for routine re-key

See chapter 3.3.

3.3.2. Identification and authentication for re-key after revocation

Penneo's CA does not support re-key after revocation.

3.4. Identification and authentication for revocation request

The requests for revocation is implemented through a request from Penneo’s authorized and responsible employee based on specified internal conditions. See 4.9.2. and 4.9.3 of the Certification Policy.

4. Service life-cycle operational requirements

4.1. Seal certificate application

4.1.1. Who can submit a certificate application

A certificate application for the issuance of the Seal certificate may be submitted by defined and authorized Penneo employees.

4.1.2. Enrollment process and responsibilities

The certificate application process for CAs belonging to Penneo starts with a written request. All information about OID and common names has to be prepared in advance and included in the request. The request is approved by Penneo's management.

It is the responsibility of Penneo's authorized employees (see section 1.5.3) to be acquainted with the certificate processes and to provide complete, accurate and true data.

Penneo's authorized employees check the data and verify the written request with Penneo's management. They follow an internal written procedure for a key pair to be generated in the hardware security module (HSM), issue the certificate, and implement the certificate in Penneo's PKI service for use in the Platform's automated process.

The private key remains saved in the HSM, which is owned and managed by Penneo. It has been installed and is being operated according to the provider's documentation.

The keys use a suitable cryptographic algorithm as defined in the standard ETSI TS 119 312.

4.2. Certificate application processing

4.2.1. Performing identification and authentication

The identification and authentication process is described in chapters above (3.2.2. and 3.2.3.) and Penneo's internal security procedures.

The identification and authentication process for Penneo’s root CA and subordinate CAs is managed by Penneo.

4.2.2. Approval or rejection of certificate application

The written request is evaluated by Penneo's management based on internal security procedures. The written request is either approved or rejected. Certificates are only issued with management approval and all such activities are documented.

4.2.3. Time to process certificate applications

Penneo's security manager will review applications in a timely manner and ensure applications are appropriately processed. The certificate is issued during 3 working days after request.

4.3 Certificate issuance

4.3.1. CA actions during certificate issuance

During the process of certificate issuance, the written request is verified and checked by Penneo's authorized employees following internal written procedure. If all controls are met, the keys are generated securely in the HSM, where the certificate is also issued. The certificate issuance process is recorded.

The process of key pair generation and certificate issuance is managed and fully automated and performed in the HSM.

4.3.2. Notification to subscriber by the CA of issuance of certificate.

Issuance of the certificate is managed by internal procedures and the issued certificate is implemented in the Platform infrastructure.

The certificate and associated private key is used during the Platform's automated process of document processing (electronic signature, seal and time stamp).

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

Penneo's auhorized employees create the certificate for the electronic seal and prepare it for automated processes of the Platform and cooperating PKI services. The process is approved by Penneo's management and defined steps are performed.

Subscribers, after all conditions of Penneo's Platform and PKI services have been met, receive signed, sealed and time stamped documents. Subscribers can verify the validity of the certificate inside the document.

4.4.2. Publication of certificate by the CA

The certificates from Penneo's CA's are published by Penneo on the website stated under 2.2.1.

Subscribers' certificates are published in the public registry.

4.4.3. Notification to subscriber by the CA of issuance of certificate

The completion of the seal certificate issuance to the Penneo A/S entity for use within the Platform's automated process is confirmed by Penneo's authorized employees managing the issuance. They confirm the result to Penneo's management.

4.4.4. Seal service agreement

The Agreement provides customers access to the Platform, enabling the subscriber to access agreed services.

The Agreement applies to delivery of the Platform and additional services from Penneo to the subscriber unless it has been expressly derogated from or modified by another written agreement and it can be established with certainty that the intention was to derogate from this agreement.

The purpose of the Agreement is to lay down the conditions for the delivery of the Platform. Customers use the Platform to request signatures from other parties. Signers (including employees of companies, organisations or other legal entities) use the Platform to sign documents using their personal certificates for electronic signature. The Platform uses Penneo's certificate for electronic seal to seal the documents upon completion of the signers' signatures.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

The private key and certificate are issued by Penneo's authorized employees according to internal procedures. The private key is saved in the hardware security module which is owned and managed by Penneo as described in the standard ETISI TS 119 431-1.

Penneo's Platform ensures that the private key can only be used under Penneo's control, as part of the Platform's automated processes.

4.5.1.1. Seal service activation

Penneo's PKI service is configured to ensure that the seal certificate can only be used to seal documents upon requests from the Platform. The Platform's automated connection to the RQSCD relies on infrastructure keys. These are only used by Penneo and installed by trusted employees following documented internal processes. The keys are restricted to the intended purpose within the system and not shared. An infrastructure key is replaced and destroyed before its algorithm reaches end of life, or if the key is suspected to be compromised.

Automated requests for sealing of documents is implemented as part of the Platform's processes:

- Penneo's customer authenticates to the Platform and prepares documents for signatures, using their web browser, Penneo's public API or another integration client.
- Each signer receives a unique link to the document(s).
- Each signer accesses the Signer Interaction Component via the link and is unambiguously identified through an RA/IP's process. Their unique subscriber ID is issued by the RA/IP is sent to Penneo's Platform as an e_token. The Platform validates to origin and content of the e_token.
- The signer agrees to the Signature Acceptance Note, thereby accepting Penneo's End User License Agreement, certificate documentation, policies and practice statements.
- The Platform generates a key pair and issues a certificate, and remote electronic signature is generated (as per separate Certificate Policy and Practice Statement for Qualified Remote Electronic Signature),
- if all subscribers sign the document, the remote sealing process is activated:
    - the Platform sends a request for Qualified Remote Electronic Seal to the PKI services cooperating with the Platform;

- the Platform verifies that all signatures are present;
- the Platform seals the document using Penneo's qualified seal certificate, seals the document, saves it to the internal database and shares it with the customer and signers. The entire process is fully automated.

The Platform does not allow subscribers to obtain and use a seal certificate for their own legal entity.

4.5.2. Relying party public key and certificate usage

A relying party may be obliged to rely on certificates mentioned in this CP which are consistent with applicable certificate content.

Relying parties are advised to download related CA certificates from Penneo's web pages and verify the content of certificates - at minimum common name, fingerprint and validity - before using subscribers' certificates. Moreover, they have to verify if the CA is qualified for trustworthy and evaluate whether the certificate issued by a subordinate certification authority pursuant to this policy is suitable for the purpose for which the certificate was issued.

4.6. Certification renewal

Certificate renewal is not provided by Penneo's trust services. Penneo always issues a new certificate.

4.7. Certificate re-key

Certificate re-key is not provided by Penneo's trust services. Penneo always issues a new certificate based on a new application and identification.

4.8. Certificate modification

Certificate modification is not provided by Penneo's trust services. Penneo always issues a new certificate.

4.9. Certificate revocation and suspension

The certificate for electronic seal is issued for a longer time period and revocation and suspension is available in the case of certain conditions being met.

4.9.1. Circumstances for revocation

Penneo's authorized employees immediately perform revocation, if:

- suspicions about misusing of private key detected in Penneo;
- decision from Penneo’s responsible manager;
- Penneo’s other conditions defined in internal documentation.

4.9.2. Who can request revocation

Penneo’s authorized employees or Penneo’s management can request revocation and start revocation process.

4.9.3. Procedure for revocation request

The request for revocation/suspension request has to be approved by Penneo's management. The automated process of remote electronic services is stopped and waiting for the new key generation and issuing of the certificate. An analysis is performed and steps for possible negative effects are removed.

A request to revoke the certificate in the future is not supported.

Penneo's manager approves issuing of the new certificate.

After issuing of the certificate:

- new private key is implemented to secure cryptographic module;
- new certificate is published;
- the Platform and cooperating PKI services are started.

4.9.4. Revocation request grace period

Revocation request must be solved for Penneo Platform services immediately.

4.9.5. Time within which CA must process the revocation request

The revocation request must be processed immediately upon receipt and approval. A new CRL has to be issued immediately after the revocation.

4.9.6. Revocation checking requirement for relying parties

Unavailability of automated process should be corrected in very short time and information about it is published via internet to all subscribers and relying parties.

4.9.7. CRL issuance frequency

The subordinates CA for electronic signature, seal and time stamp issues CRL every 12 hours, with validity time 24 hours.

4.9.8. Maximum latency for CRLs

CRLs of subordinates CA for electronic signature, seal and time stamp are always issued no more than 12 hours after the issuance of the previous CRL.

4.9.9. On-line revocation/status checking availability

OCSP is not used.

4.9.10. On-line revocation checking requirements

OCSP is not used.

4.9.11. Other forms of revocation advertisement available

Other forms are not supported.

4.9.12. Special requirements re-key compromise

The process is the same as during the revocation request.

4.9.13. Circumstances for suspension

Not supported.

4.9.14. Who can request suspension

Not supported.

4.9.15. Procedure for suspension request

Not supported.

4.9.16. Limits on suspension period

Not supported.

4.10. Certificate status services

4.10.1. Operational characteristics

Penneo’s Root and Subordinated CA’s are published and available on Penneo’s web pages.

Subscribers’ certificates are published in the public registry.

CRLs are regularly issued and published on Penneo's web pages.

Certificates contain information about a subscriber’s personal information and the certificate usage.

The complex processes of certificate status verification are performed by the Penneo Platform and are fully automated without interruption.

4.10.2. Service availability

Penneo’s services (the Platform and CAs) are available 24×7. Everything is performed way without interruption. CRL is available on addresses defined in certificates.

4.10.3. Optional features

Optional features are not provided.

4.11. End of subscription

Penneo’s CA issuing certificates for subscribers (physical or legal), performs qualified services and is responsible to perform the all promised activities mentioned inside CPS and/or this CP for the all time period of certificates are valid (for the period of validity of the last issued Certificate).

Subscriber's certificates have short validity time and process of validity verification is managed by internal Platform procedures.

Conditions and rules are described in internal Key management documentation.

Subscription period for access and usage of the Platform is defined by the agreement between Penneo and customers. Either Party may terminate the customer Agreement according to the terms of the contract and the Data Act. If

the Agreement is not terminated at the latest 3 months before the expiry of the subscription period, this gives rise to a new subscription period of 12 months.

The End User License Agreement defines access and usage of the Platform for signers.

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery police and practices

Penneo does not use key escrow services.

4.12.2. Session key encapsulation and recovery policy and practices

Penneo uses hardware security modules and procedures defined by the supplier for completion of the CA keys during recovery. Parts of keys are encrypted and cannot be transfered in readable form. After activation the private key never leaves the secure cryptographic environment.

5. Facility, Management, and Operational Controls

📌 This document does not bring any additional information to the Facility, Management, and Operational Controls. For relevant information please see chapter 5 of Trust Service Practice Statement.

6. Technical Security Controls

6.1 Key pair generation and installation

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.1 of Trust Service Practice Statement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2 of Trust Service Practice Statement.

6.3 Other aspects of key pair management

This document does not bring any additional information to this chapter. For relevant information please see chapter 6.3 of Trust Service Practice Statement.

6.4 Activation data

This document does not bring any additional information to this chapter. For relevant information please see chapter 6.4 of Trust Service Practice Statement.

6.5 Computer security controls

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.5 of Trust Service Practice Statement.

6.6 Life cycle technical controls

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.6 of Trust Service Practice Statement.

6.7. Network security controls

Penneo's root CA is not accessible to subscribers and the status is off-line. The rest of Penneo’s services, which is through subordinate CA’s are accessible via the internet but protected through numerous security measures like network segmentation to ensure that the Platform is logically separated other resources is access is restricted to only authorised persons.

The same security controls are applied on all systems within one zone.

Trust Service components must be kept in a separate zone and especially system critical components for the TSP (such as Root CA) are kept in (one or more) secured zone.

All connections that are not needed for the service operated in the production environment must be deactivated / blocked, i.e. a deny by default policy must be applied. This also means that access and communications between zones for TSP operations are restricted to only those necessary.

Communication between trustworthy systems is running only through trusted channels. These channels are isolated physically from other communication channels. These measures provide guaranteed identification of their endpoints and protect the channel data against modification or disclosure.

Transfer of data between registration authorithies are performed via encrypted communication between Penneo’s services is through secure internet channel (protocols https and mTLS).

7. Certificate, CRL, and OCSP Profiles

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 7 of Trust Service Practice Statement.

8. Compliance Audit and other Assessments

This document does not bring any additional information to this chapter. For relevant information please see chapter 8 of Trust Service Practice Statement.

9. Other Business and Legal Matters

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 8 of Trust Service Practice Statement.

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Christel Victoria Høst
PENNEO A/S CVR: 35633766
Chief Operating Officer
Serial number: 66d16c3a-ebd4-4bba-beb5-6d4299861cb9
IP: 2.106.xxx.xxx
2026-01-08 05:26:37 UTC