PS for Remote Electronic Signature with Remote QSCD

Version	Valid from	Approved by (Title and name)	Comments
1.3	28.01.2026	COO / Christel Victoria Høst	Corrected X.501 to X.509 under 3.1.1.
1.2	08.01.2026	COO / Christel Victoria Høst	Details about Penneo's qualified remote signing 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. 1.3.2, 4.2, 4.5.1.1 Included possibility of different clients. 4.7 Certificate re-key not supported. 4.9.7 CRL validity and frequency
1.1	27.12.2024	Information Security Manager / Fredrik Lernevall	Improved readability. Updated Certificate application processing 4.2 and subsections. Initial identity validation 3.2. Certificate life-cycle operational requirements 4.1.1 - 4.5.2
1.0	22.11.2022	Information Security Manager /	First release

		Fredrik Lernevall	

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 Signature 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 Signature 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 signature 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. Document name and identification

Name and Identification of the document:

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

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

Penneo’s Platform, including RQSCDs and applications, provides qualified electronic signatures to identified subscribers (customers/signers) through a fully automated process, via a Registration Authority/Identity Provider service.

The remote qualified electronic signature service is provided by Penneo and accessed by subscribers (customers/signers) through the Signer Interaction Component (SIC) via their web browser. The agreement between Penneo and the customer is described in Penneo’s Terms and Conditions.

The Services of remote qualified electronic signature involve several actors:

- **Customers** - means a company, organisation or other legal entity that has accepted Penneo's Terms, as part of entering an agreement with Penneo, either directly or by accepting the Penneo Order Confirmation.
    - A customer authenticates on the Platform, then uploads documents for electronic signature and adds details of signers, using Penneo's web application, public API or other integration client.
    - Send an invitation to sign with a unique link to the SIC to each signer, via email or other appropriate client.

  Note: These Customer's activities are out of scope, as far as the applicable standards for Penneo's qualified trust services are concerned. They are included for completeness and understanding of the broader process through which the qualified remote signing service is available to subscribers.

- **Signers** (could be employees working on behalf of the Customer’s company, organization or other legal entity, employees of other Customers or other natural persons) - receive a request for signature via email or other appropriate client, containing a unique link to the Platform. Signers are not necessarily Penneo's customers but they enter an agreement with Penneo by accepting Penneo's End User License Agreement through the SIC before they sign.
    - Upon receipt of the signature request, the signer accesses the SIC via the link, reads the document(s) and selects an approved Registration Authority. The Platform initiates a session with the RA. The signer completes the RA’s process for identification and authentication, and the RA sends an e_token to the Platform containing the signer’s unique ID data.
    - The Platform validates the returned e_token, its subscriber ID data, assurance level and origin to determine whether the certificate to be issued can be Qualified.
    - A Signature and Acceptance note is displayed to the Signer for approval alongside the data to sign, legal conditions and information about Penneo’s qualified trust services.
    - The signer verifies all data and confirms. The remote signing process starts. A key pair generated in the Remote Qualified Signature Creation Device (RQSC) is assigned to the signer, and the signer’s certificate is issued.
    - Once the remote electronic signature process is finished, the Platform uses Penneo’s certificate for electronic seal to seal the document. The final document is sent to all signers and the Customer.
    - The process of certificate application is fully automated and carried out inside the Platform.
- **Penneo** as qualified trust service provider through the Platform:
    - Operates and is responsible for the Platform availability including the Public Key Infrastructure (PKI) services and Remote Qualified Signature Creation Device;

    - Issues certificates to subscribers through its subordinate CA for remote electronic signature;
    - Is responsible for customers/signers through approved Registration Authority/Identity Provider services;
    - Provides qualified remote services, including certificates, seals, signatures and timestamps;
    - Uses external parties for the Platform implementation.

1.3.3. Registration authorities

Registration authorities (RA) are external companies (third parties) and their activities, among others are:

- To perform subscriber identification and authentication according to well-defined activities and procedures.
- To provide a unique identifier (subscriber ID) to each subscriber.
- To save subscribers identification information to their databases.
- To send the subscriber's ID data as an e_token, signed by their key, and following the OpenID Connect protocol, upon remote request from the Platform for subscriber verification.

Information about approved RAs is published in CP for Qualified Remote Electronic Signature Certificate.

1.3.4. 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 signature of the signers based on the CA's hierarchy.

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

1.3.5. Other participants

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

- Registration Authorities in the role of Identity Providers,
- Data centre services,
- Hardware suppliers,
- Software suppliers,
- Cloud solution provider,
- Time synchronisation service 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. Certificate usage

1.4.1. Appropriate certificates uses

A subscriber's Certificate issued by Penneo under the Certificate Policy and Practice Statement may be used for qualified remote electronic signature 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

Subscribers are named according to their ID information provided to Penneo by an approved Identity Provider, which perform procedures as Registration Authority.

3.1.1. Types of names

The structure of naming conventions is implemented in accordance with the scheme of the X.509 standard (resp. X.520 standard), valid standards and directives.

3.1.2. Need for names to be meaningful

Penneo receives the subscriber's name from the RA/IP, who has validated the name using an official authoritative source, as described in their published practices and according to internally accepted standards.

3.1.3. Anonymity or pseudonymity of subscribers

Anonymity or pseudonymity is not 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

When the subscriber is registered through the RA/IP's process, a unique identifier (subscriber ID) is created. When verification of the subscriber is initiated through Penneo's digital signature Platform, the RA/IP sends an electronic token (e_token) to the Platform. The e_token contains both the subscriber ID and name details. The Platform inserts this in the subscriber's certificate being issued by the Platform, thereby ensuring uniqueness of names in certificates.

3.1.6. Recognition, authentication, and role of trademarks

The Platform is operated by Penneo, which has registered the name a trademark. Subscribers may use the Platform but shall respect the intellectual property rights.

The subscriber accepts the End User License Agreement, which explicitly states that the Platform and the Penneo name are protected by intellectual property rights, and that they as subscriber are liable for any misuse of such.

3.2. Initial identity validation

The initial process of identity verification and validation is performed through defined rules and procedures of so named Identity Providers which perform procedures as Registration Authorities (RA/IP) for the Penneo Platform.

RAs/IPs implement the processes for subscriber identification and sends a signed electronic token (e_token) to Penneo containing the subscriber's validated identity data.

The subscriber can only use approved RA/IP services, as described in CP for Qualified Remote Electronic Signature Certificate.

The certificate must be issued within 15 minutes from issuance of the e_token, otherwise the Platform will reject the request and the subscriber will need to repeat the RA/IPs process and submit a new application.

3.2.1. Method to prove possession of private key

Private key ownership is realized through the following process:

- The subscriber is unambiguously identified through an RA/IP's process. Their unique subscriber ID issued by the RA/IP is sent to Penneo's Platform as an e_token following the OpenID Connect protocol, if the verification is successful. The Platform validates the origin and content of the e_token.
- The subscriber ID is used by the Platform as input for an automated process.
- Before allocation of a key pair and issuing of a certificate, the subscriber confirms their name as provided by the RA/IP and agrees to the Signature Acceptance Note, thereby accepting Penneo's End User License Agreement, certificate documentation, policies and practice statements.
- The Platform communicates with the PKI services as described in internal processes in order to generate a key pair and a certificate. This process is fully automated and remote. The private key is managed using a Remote Qualified Signature Creation Device.
- The subscriber can exclusively use the private key and certificate for the automated process of remote qualified signature creation through the Platform within a given signing session.

3.2.2. Authentication of organizational identity

Penneo only issues certificates for remote electronic signature to natural persons. The Platform does not allow subscribers to obtain a certificate linked to their company’s legal entity.

3.2.3. Authentication of individual identity

Identification and authentication of individual identity (customer/signer) is performed by a RA/IP. A RA/IP uses processes and means supporting unambiguous identification and authentication according to law and EU regulation before issuing a subscriber's ID identifier. Without an issued subscriber's ID it is not possible to start the remote and automated process of the Platform for qualified remote electronic signature.

3.2.4. Non-verified subscriber information

The RA's procedures for subscriber ID verification include error handling when the subscriber's attempt to complete the identification is unsuccessful. The RA limits how many times a subscriber can re-try within a given session.

If the subscriber does not complete the RA's process, an error is shown when they return to the Platform and they cannot continue the process. The same is true if the Platform cannot verify the subscriber ID information in the e_token, or the validity of the e_token itself.

In both cases the subscriber will need to initiate a new session and repeat the RA's procedure from the start.

For more information about non-verified subscriber's information see the documentation of the particular RA/IP.

3.2.5. Validation of authority

Penneo's PKI services use the subscriber's ID identifier and further data from the corresponding subscriber's electronic token (e_token) when assigning a key pair and issuing a certificate, as part of an automated remote process for electronic signature creation via internet connection.

Validation of Penneo's CA is performed through defined application processes through CA hierarchy verification. Penneo's organizational entity is included in each certificate together with the subscriber's identity.

The certificates of the subordinated CAs are implemented in the Platform's application processes which perform activities for electronic signature based on Penneo's CA hierarchy.

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

A subscriber's certificate is issued for a one time process only and for a time limited period. It can only be used within the same signing session where it is issued. Certificate revocation and suspension is not supported.

4. Certificate/signing key life-cycle operational requirements

4.1. Certificate application

4.1.1. Who can submit a certificate application

An application for a remote electronic signature certificate may be submitted automatically via internet connection by a subscriber (natural person), as part of the process of signing a given document. The subscriber must have completed the identification processes of the RA/IP within the last 15 minutes during the particular document signing session. The subscriber must accept Penneo's End User License Agreement (EULA) and agree to sign the given document(s).

4.1.2. Enrollment process and responsibilities

The certificate’s subscriber is responsible for reading this PS and other public documents regarding Penneo’s electronic signature service and certificate usage, including the CPS and trust service practice statements.

A RA/IP has to verify the completeness and accuracy of a subscriber’s data and issue a unique subscriber’s ID identifier.

It is the responsibility of the RA/IP to maintain up-to-date information of the subscriber's identity and to provide adequate and accurate data to the Penneo Platform.

The certificate is issued based on the subscriber’s ID verification using the data provided in the e_token.

The process is fully automated and conducted via internet communication (via the subscriber’s web browser) between the Platform and the particular RA/IP.

Before the remote signature process can start, the subscriber has to

- read the document(s) to be signed;
- be verified and authenticated;
- confirm personal data;
- agree to Penneo's End User License Agreement and further policies shown as a Signature and Acceptance note;
- express intention to sign the document(s).

Penneo, as operator of PKI services, is required to:

- publish the Root CA certificate and Subordinate CA certificates that are part of the Penneo Platform’s automated remote processes;
- publish all public documents and policies of CA services.

4.2. Certificate application processing

Processing of subscriber’s certificate request is divided into several parts:

- Penneo's customer authenticates to the Platform and prepares documents for signatures, using their web browser, Penneo's public API or another integration client.
- The signer (subscriber) receives a unique link to the document(s).
- The signer accesses the SIC via the link and reads the document(s). The signer's web browser is used.
- A list of supported Registration authorities/Identity providers is displayed. The signer selects an approved RA/IP, the Platform initiates a session with the RA/IP, and the signer completes the RA/IP's process.
- The RA/IP sends an e_token to the Platform containing the signer's unique ID identifier and personal data. The Platform validates the returned e_token, its subscriber ID data, origin and assurance level to determine whether the certificate to be issued can be Qualified.
- Using the signer's web browser, the a Signature and Acceptance note is displayed to the Signer for approval alongside the data to sign, End User License Agreement and information about Penneo's qualified trust services.
- The signer verifies all data and confirms their intention to sign. The remote signing process starts. Key pairs generated in the RQSCD are assigned and the signer's certificate is issued.
- Once the subscriber has confirmed their intention to sign, the process of certificate application is fully automated and carried out inside the Platform without any interaction.

4.2.1. Performing identification and authentication

Identification and authentication of the subscriber for CA services is performed by an approved RA/IP under contract with Penneo.

- The Platform initiates a session with the RA/IP.
- The subscriber completes the RA/IP's process for identification and authentication, and the RA/IP sends an e_token to the Platform containing the signer's unique ID identifier and personal data.

- The Platform validates the returned e_token, including the assurance level, that its data is signed by an approved RA/IP and that it has not expired,to determine whether the requirements to issue a Qualified certificate have been met.

If the identification and authentication phases are successful the subscriber can continue in following phases of remote electronic signature.

4.2.2. Signing key generation

Key pairs for the subscribers' certificates are generated in the Remote Qualified Signature Creation Device (RQSCD) operated by Penneo, which is certified according to EU regulation and applicable technical standards, as further described in CP for Qualified Remote Electronic Signature Certificate.

A hardware security module (HSM) is part of the RQSCD, which also uses a certified Signature Activation Module as per the standard CEN EN 419 241-2. It 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.

Subject to all conditions for subscriber identification and key generation being met, the subscriber's certificate is issued based on data from the e_token. The process of certificate creation and CA activities is fully automated and performed in the HSM.

Once the certificate has been issued, the automated remote signing process continues.

The automated connection to the RQSCD relies on infrastructure keys. These are only used by Penneo and installed by trusted employees following documented internal processes. They 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.

4.2.3. Approval or rejection of certificate application

The RA’s procedures for subscriber ID verification include error handling when the subscriber’s attempt to complete the identification is unsuccessful. The RA limits how many times a subscriber can re-try within a given session.

If the subscriber does not complete the RA's process, an error is shown when they return to the Platform and they cannot continue the process. The same is true if the Platform cannot verify the subscriber ID information in the e_token, or the validity of the e_token itself as described in 4.2.1.

In these cases the subscriber will need to initiate a new session and repeat the RA's procedure from the start.

4.2.4. Time to process certificate applications

The certificate issuance begins immediately and is completed within seconds, once the subscriber has completed the RA/IP's process and confirmed the intent to sign the document(s), and once the automated validation that all requirements have been met is completed.

4.2.5. eID means linking

During the signing process, a list of approved RA/IPs is displayed. Based on the subscriber's selection, the Platform initiates a session with a particular RA/IP, and the subscriber confirms his/her identity via their process remotely.

After successful identity confirmation, the RA/IP sends an electronic token (e_token) to the Platform containing the signer's unique ID identifier and personal data. This e_token is used for the Platform's automated process for certificate issuance and remote signature creation.

The process of the subscriber's e_token validation and usage is fully automated and takes place via the web application and web browser.

4.2.6. eID means provisions

Penneo uses the unique ID identifier and personal data received from the RA/IP in an e_token to issue a certificate for remote electronic signature.

Penneo does not itself provide eID means.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

The process of key pair generation and certificate issuance is fully automated. It is conducted by the Penneo Platform's software using a Remote Qualified Signature Creation Device (RQSCD) with a hardware security module (HSM) as described in 4.2.2.

The Penneo platform creates a session with RA/IP for the subscriber via internet connection. Through this connection, the Platform receives an e_token from the RA/IP.

Once the Platform has verified that the requirements for subscriber ID validation have been met and keys have been generated and assigned, as described in 4.2.1 and 4.2.2 respectively, the Platform creates a certification request containing the subscriber ID data from the e_token, signs it with the subscriber's private key, and issues the subscriber's certificate. The certificate is signed with the issuing CA's private key and stored in the RQSCD operated by Penneo, where also the subscriber's private keys remain.

All hardware and software used in this process is deployed in a secure environment, the RQSCD is tamper-proof, and the steps for key generation and certificate issuance can only be initiated by the Platform's software

The validity of the subscriber's certificate will be 1 day as per the CP, and it will never be valid for longer than the issuing CA, since a new issuing CA will be issued well in advance of the expiry of the current issuing CA.

As soon as the certificate has been issued, the automated process of remote electronic signature creation continues.

4.3.2. Certificate linking

Certificate linking with the subscriber's private key is performed through the Platform. The linking happens during the subscriber's signing session, where the certificate is issued, and the private key can only be used with the issued certificate.

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

The certificate is issued as part of a document signing process, and subscribers are notified of the issuance of a certificate during the signing process. After identification with the RA/IP, when the e_token has been obtained, a Signature and Acceptance note is shown to the subscriber in their web browser. The Platform ensures that the subscriber confirms their intention to sign before the certificate issuance and signature creation begins.

Upon completion, the subscriber is informed that the signature has been created, implying that the certificate has been successfully issued.

4.4. Certificate acceptance

By accepting to sign a document, the subscriber accepts Penneo's End User License Agreement (EULA), as per the Signature and Acceptance note presented during the signing process. As part of the generation of a remote electronic signature, they accept the certificate issued, and that Penneo manages the keys on their behalf. The subscriber also accepts that Penneo's certificates are used to generate qualified timestamps, and a qualified seal for the signed document.

The full EULA is available to the subscriber alongside Penneo's qualified trust service documentation, and the subscriber's acceptance is included in the data to be signed.

The subsequent process is fully automated. The CA services use the confirmation to perform the next steps of the certificate processing. The subscriber is informed about each step of the process via the Penneo Platform in their web browser.

4.4.1. Conduct constituting certificate acceptance

The acceptance of subscribers certificate is a fully automated process and it is part of the Platform. Certificates of CAs services are accepted during initialization phases of key generation and certificate issuance.

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 services of key generation, certificate issuance and notification that the certificate is provided to the subscriber is based on an automated process of Penneo Platform and CA services.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

The subscriber’s private key and certificate are issued during a specific signing session for one time use. The private key is deleted after the electronic signature is created. If the subscriber needs to complete multiple signing processes, separate keys and certificates will be issued each time, subject to the subscriber's repeated identification and acceptance.

The subscriber's private key is stored in the Remote QSCD's hardware security module and managed by Penneo on their behalf as described in the standard ETSI TS 119 431-1. Penneo's Platform and processes ensure that the private key can only be used under the subscriber's sole control, as part of the signing session in which the corresponding certificate is issued.

The subscriber’s responsibility are:

- usage of the private key and certificate according to processes mentioned in this CP;
- usage of the private key and certificate according to relating legal purposes only;
- be informed in advance about electronic signature functionality and necessary steps to be fulfilled.

Subscribers have to inform Penneo’s contact places immediately, if:

- suspicion about misuse of a private key or inappropriate the Penneo Platform behaviour arises;
- data in the certificate is not complete or accurate. If the information is inaccurate, the subscriber has to send the information to Penneo contact points and arrange a new registration process.

4.5.1.1. Signature activation

The Customer:

Note: These Customer's activities are out of scope, as far as the applicable standards for Penneo's qualified remote signing service are concerned. They are included for completeness and understanding of the broader process through which the qualified remote signing service is available to subscribers.

- is verified in the Platform and prepares one or more documents for signature. Process is managed by Web application, public API or another integration client;
- defines the list of signers necessary for document signature and sends invitation to signers via e-mail or other appropriate client.

The Signer:

- Uses the unique link included in the e-mail application or other channel to view the document(s) via Web application (WYSIWYS).
- After getting acquainted with the content of the document, they can start the signing process.
- Is obliged to identify and authenticate themself, through internet communication with RA, who will issue the Subscriber ID as an e-token to the Platform.
- Confirms their intention to sign the document(s), and agreement to the Signature and Acceptance note, including legal conditions. The automated process managed by Penneo follows.

Penneo:

- Creates a new signing session for each signer for each (set of) document(s)
- Creates a new session with an approved RA for identification of the subscriber within the specific signing session.
- Validates the e_token received from the RA, to ensure that all requirements for issuance of qualified certificates and signatures are fulfilled.
- Approves all RAs available in the Platform for subscribers requesting a qualified electronic signature, by ensuring the RAs are compliant with article

24.1 of the eIDAS regulation, and integrated according to their documentation and applicable standards.

- Obtains the subscriber's agreement to the signature creation, as well as the End User License Agreement, and applicable terms and policies, before commencing the qualified remote signing process.
- Creates a key pair in the RQSCD, assigns it to the subscriber, and ensures that it can only be used within the signing session.
- Generates Signature Activation Data (SAD) under the subscriber's sole control during the Signature Activation Protocol (SAP), uniquely linked to the subscriber's ID information provided in the e_token from the RA. The SAD describes the Data To Be Signed (DTBS).
- Sends the SAD to the Signature Activation Module (SAM) following the SAP, so that the SAM can verify its integrity and content, including DTBS, subscriber information and key to be used.
- Maintains the signing session, thereby ensuring that the key is always linked to the subscriber, and to the given SAD, DTBS and SAP.
- Issues certificate with short-term validity, to be used only in the specific signing session, and ensures that the certificate is valid at the time of signing.
- Issues a qualified electronic time stamp for the signature, as described in PS for Time Stamp Authority.

In the case that more than one signer is to sign the document(s), each signer completes the signing process as a subscriber independently of the other signers. The Platform collects all signatures, and after the last signature the document(s) are sealed and distributed to all signers and the Customer. The sealed document contains all signature certificates and is locked for editing.

4.5.1.2. Signing key deletion

The subscriber’s private key and certificate usage is a one time process only. After the electronic signature is created, the subscriber’s private key is deleted by the Platform and HSM.

4.5.1.3. Signing key backup and recovery

Backup and recovery of signing keys is not provided by Penneo. The keys are for single use only.

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.

4.5.3. Signature creation application services component technical requirements

The Platform's front end is the application running in the subscriber's browser. Subscriber through the Web sends requests for the Penneo Services and interacts with the Platform.

Interaction is split into 4 logical flows:

1. Authentication flow.
2. User signing flow.
3. Validation flow.
4. Sealing flow.

Subscriber interacts in:

- Authentication flow.
- User Signing Flow.

Before the subscriber can sign any document, identification and authentication must be successfully performed, and a valid subscriber authorization e_token has to be sent to the Platform by the RA/IP.

The Platform validates the completed signatures, including their certificates, before concluding the signing process. Only validated signed data can be stored in the database. This is also confirmation that the signing process has been done correctly and no manipulation with the signed data happened.

The document is finalized (signed and sealed) when all required signers have signed the document. The resulting document contains all signed information with possibility to check and verify subscribers , time stamps and seal and it is distributed to all signers and the customer.

4.5.4. AdES digital signature creation

Digital signature is created inside the HSM.

4.6. Certificate renewal

A subscriber’s certificate renewal is not provided by Penneo's CAs services. The CAs always issues a new certificate.

4.6.1. Conditions under which certificate renewal takes place

See chapter 4.6.

4.6.2. Who may request certificate renewal

See chapter 4.6.

4.6.3. A CA or RA’s procedure to process renewal request

See chapter 4.6.

4.6.4. Notification of the certificate to the subscriber

See chapter 4.6.

4.6.5. Conduct constituting acceptance of the certificate

See chapter 4.6.

4.6.6. Publication of the certificate by the CA

See chapter 4.6.

4.6.7. Notification of certificate issuance by the CA to other entities

See chapter 4.6.

4.7. Certificate re-key

Certificate re-key is not supported by Penneo's trust services. Penneo always issues a new certificate based on a new RA/IP session.

4.8. Certificate modification

The CA always issues a new certificate based on previous identification and authentication of subscribers (with subscriber ID usage) in approved RA/IP.

4.8.1. Conditions under which certificate modification can take place

See chapter 4.8.

4.8.2. Who may request certificate modification

See chapter 4.8.

4.8.3. A CA or RA's procedure to process modification request

See chapter 4.8.

4.8.4. Notification of the certificate to the subscriber

See chapter 4.8.

4.8.5. Conduct constituting acceptance of the certificate

See chapter 4.8.

4.8.6. Publication of the certificate by the CA

See chapter 4.8.

4.8.7. Notification of certificate issuance by the CA to other entities

See chapter 4.8.

4.9. Certificate revocation and suspension

A subscriber's certificate is issued for a one time process only and for a time limited period. It can only be used within the same signing session where it is issued. Certificate revocation and suspension is not supported.

CPS and CP for Root and Intermediate CA contains information about revocation of Penneo's Root CA and the subordinary CA used to issue subscribers' one-time certificates.

4.9.1. Circumstances for revocation

see Chapter 4.9.

4.9.2. Who can request revocation

see Chapter 4.9.

4.9.3. Procedure for revocation request

see Chapter 4.9.

4.9.4. Revocation request grace period

see Chapter 4.9.

4.9.5. Time within which CA must process the revocation request

see Chapter 4.9.

4.9.6. Revocation checking requirement for relying parties

see Chapter 4.9.

4.9.7. CRL issuance frequency

The Root CA of Penneo's services issues CRL no more than 180 days after the issuance of the previous CRL with validity time 180 days.

Subordinate CAs issue the 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

Certificates for electronic signature are issued with time limited period. Other forms are not supported.

4.9.12. Special requirements re-key compromise

Special requirements re-key compromise are not supported.

4.9.13. Circumstances for suspension

Penneo's CA services do not support suspension of subscribers certificates for electronic signature.

4.9.14. Who can request suspension

Penneo's CA services do not support suspension of subscribers certificates for electronic signature.

4.9.15. Procedure for suspension request

Penneo's CA services do not support suspension of subscribers certificates for electronic signature.

4.9.16. Limits on suspension period

Penneo's CA services do not support suspension of subscribers certificates for electronic signature.

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

Services of Penneo’s PKI are available 24 hours a day, 7 days a week. CRLs are available on addresses defined in certificates.

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.

Penneo ensures accessibility to the Platform during the term of the Agreement is uptime of 99.9%

The uptime is measured and calculated per calendar month based on service time 24/7. In the calculation of uptime, downtime of which notice has lawfully been given in pursuance of the Agreement or which has otherwise expressly been accepted by the subscriber is not included.

The subscriber can at any time see the status of Penneo’s uptime at status.penneo.com.

4.10.3. Optional features

CRLs are available 7 days a week, 24 hours.

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.

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

6.1.1 Key pair generation

> 📌 This document does not bring any additional information to the Key pair generation. For relevant information please see chapter 6.1.1 of Trust Service Practice Statement.

6.1.2 Private key delivery to subscriber

Private keys are saved in the hardware security module of the RQSCD. They are managed by Penneo on the subscriber's behalf and can only be used under their sole control through the SAP within the signing session.

6.1.3 Public key delivery to certificate issuer

Not relevant. For subscribers, the key pair generated and stored in the hardware security module. The public key is part of the certificate and used by the Platform for validation of the electronic signature.

6.1.4 CA public key delivery to relying parties

The certificates are part of signed documents and it is possible to verify them by digital signature validation mechanisms, according to technical standards.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

> 📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2.1 of Trust Service Practice Statement.

6.2.2 Private key (n out of m) multi-person control

> 📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2.2 of Trust Service Practice Statement.

6.2.3 Private key escrow

> 📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2.3 of Trust Service Practice Statement.

6.2.4 Private key backup

Subscribers private key has no backup. They are generated and processed only once.

6.2.5 Private key archival

Private key for subscribers are not archived. They are generated and processed only once. For next signature has to be a new key pair generated.

6.2.6 Private key transfer into or from a cryptographic module

It is not relevant for subscribers.

6.2.7 Private key storage on cryptographic module

> 📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2.7 of Trust Service Practice Statement.

6.2.8 Method of activating private key

Subscribers private keys are activated by remote Penneo Platform during signature automated processes.

6.2.9 Method of deactivating private key

Deactivation of subscriber's private key is managed by automated Penneo Platform. If signing process ends correctly and documents are electronically signed the subscriber's private key is deleted by the Penneo Platform.

6.2.10 Method of destroying private key

Destroying of subscriber’s private key is managed by Penneo Platform. The private key is used only once.

6.3 Other aspects of key pair management

6.3.1 Public key archival

> 📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.3.1 of Trust Service Practice Statement.

6.3.2 Certificate operational periods and key pair usage periods

Subscriber certificate operational period is defined in the certificate .

There is no difference between operational and key pair usage period. The last subscriber’s certificate will be issued in date prior to expiration of the CA’s certificate.

Validity time of private key and corresponding public key located in certificates is the same.

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.

PENNEO

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: 93.165.xxx.xxx

2026-01-28 14:25:44 UTC

MitID

Penneo document key: CJ25Z-NOU45-39P9U-YZ1MY-VXQY8-QSDAB