CP for Qualified Remote Electronic Signature Certificate

Version history

Version	Valid from	Approved by (Title and name)	Comment
1.9	28.01.2026	COO / Christel Victoria Høst	Corrected X.501 to X.509 under 3.1.1, 7.1 basic certificate fields #4 + #8, 7.2 field #3.
1.8	08.01.2026	COO / Christel Victoria Høst	General re-wording and alignment with standard terminology throughout the document for clarity and consistency. 1.6. updated accordingly. Details about Penneo's qualified remote signing service and EULA for signers. 1.3.3, 4.2 Included possibility of different clients. 1.3.2 Added AusweisApp and approval of RAs. 1.3.5 Elaboration of other participants. 2.3 and 4.9.7 CRL validity and frequency. 4.7 Certificate re-key not supported. 9.8 Updated sum for limitation of liability.
1.7	26.11.2025	COO / Christel Victoria Høst	Minimum RSA key size changed from 2048 to 3072 for subscribers certificates under 6.1.5 and size of SubjectPublicKey under 7.1.
1.6	17.10.2025	COO / Christel Victoria Høst	Updated RSA key size for subordinate certificates under 6.1.5. Specified that size of SubjectPublicKey listed under 7.1 is minimum size.
1.5	26.05.2025	COO / Christel Victoria Høst	Updated company address under 2.2.1
1.4	14.01.2025	Fredrik Lernevall / Information Security Manager	Adding “Mandatory / Optional / Critical” column to profile in chapter 7
1.3	13.01.2025	Fredrik Lernevall / Information Security Manager	Updated validity notAfter field
1.2	23.12.2024	Fredrik Lernevall / Information Security Manager	Improved readability. Updated contact persons under 1.5.2 Updated Certificate application processing 4.2 and subsections. Retention period under 5.5.2 and 6.3.1 Initial identity validation section 3.2 Certificate life-cycle operational requirements 4.1.1 - 4.5.2
1.1	23.01.2023	Fredrik Lernevall / Information Security Manager	Updated URL for Penneo’s Trust Center under section 2.2.1

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Version	Valid from	Approved by (Title and name)	Comment
1.0	22.11.2022	Fredrik Lernevall / Information Security Manager	First draft

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Introduction

This Certification Policy (hereinafter CP) describes the principles of Penneo A/S (hereinafter as Penneo) in issuing qualified certificates for remote qualified electronic signatures to subscribers.

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 PKI services are offered to subscribers on the basis of a concluded contractual relationship between Penneo and Registration Authorities/Identity Providers.

Certificates issued in accordance with this certification policy may only be used to create and verify remote and qualified electronic signatures in accordance with applicable law.

The private key corresponding to the public key in the certificate issued under this certification policy is generated to create a remote and qualified electronic signature.

For all qualified certificates issued by Penneo's CA, the term Certificate is used.

Penneo implements its PKI infrastructure in Penneo's application (the Platform), which is built using devices owned by Penneo and hosted in a co-location data centre combined with services hosted in a public cloud environment. Both the co-location hosting provider as well as the public cloud hosting provider are certified and regularly audited and fulfil the conditions and requirements of eIDAS regulation and relevant technical standards.

1.1. Overview

The document is divided into nine chapters:

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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 2 - describes the role of the repository, the responsibilities for publishing information, time frequency of publication, and repository approaches and accesses.

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 5 - describes the principles of physical, procedural and personnel security, audit activities and logged events.

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.

Chapter 7 - describes certificate profiles and CRL profiles.

Chapter 8 - describes the area of compliance audit, assessment and evaluation of the provided services.

Chapter 9 - describes topics of financial and legal requirements, fee policy, termination of CA activities and other requirements.

1.2. Document name and identification

Name and Identification of the document:

Certification Policy for issuing qualified certificates for remote electronic signature (algorithm RSA).

OID of Policy: 1.3.6.1.4.1.57006.1.2.10.1.1

1.3. PKI Participants

1.3.1. Certification authority

Penneo has implemented a two-tier CA structure. Self-signed certificates for Root CA and certificates for subordinate CAs.

The Root CA issues certificates for:

- Subordinate Time Stamp Authority (TSA) and
- Certification Authority for remote electronic signature and electronic seal.

1.3.2. Registration Authority

In accordance with the provisions of this CP, Penneo uses services of external companies in the role of Registration Authorities (RA).

These registration authorities perform well-defined activities and procedures for subscribers' registration process, subscribers' identification and authentication and provide subscribers a unique identifier (subscriber ID). The subscriber ID is used by Penneo's digital signature platform. The RAs are acting in the role of Identity providers (IP).

For the issuance of qualified certificates, the RAs fulfill the requirements of eIDAS art. 24.1 - either as Notified electronic identification means with High level of assurance (LoA) (as per eIDAS art. 9), or as other identification methods, which ensure the identification of the subscriber with a high level of confidence, the conformity of which has been confirmed by a conformity assessment body.

For the issuance of non-qualified certificates, the RAs fulfil the requirements of eIDAS art. 26.

RAs include:

- Belgian eID - https://eid.belgium.be/ - Notified eID at LoA High

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- Norwegian BankID - https://bankid.no/ - Notified eID at LoA High and Substantial
- Danish MitID - https://www.mitid.dk/ - Notified eID at LoA High and Substantial using a dedicated hardware token or mobile app + pin code
- ID Verifier - https://ingroupe.com/product/id-verifier/ - smartphone app verifying the subscriber's identity using their NFC enabled passport and face verification, conformity assessed by a CAB
- German eID through AusweisApp - https://www.ausweisapp.bund.de/home - Notified eID at LoA High
- Swedish BankID - https://www.bankid.com/ - Notified eID at LoA Substantial

The authentication method will depend on the given RA and can include a mobile app, physical smartcard, pin code, token or a combination of these.

Other RAs that fulfill the requirements of eIDAS can also be used. Each RA is approved by Penneo before it is integrated in the Platform, by inspecting its documentation and Notified status or CAB certification, as well as relevant documents. All RAs are reviewed periodically and at least annually to ensure they continue to meet the requirements.

Penneo accesses the RA services through Broker platforms, based on bilateral contracts:

- E-Ident, provided by IN Groupe (formerly Nets) - https://ingroupe.com/product/e-ident/
- IN Groupe Signaturgruppen -https://www.signaturgruppen.dk/

1.3.3. Subscribers

Penneo's subordinate CA for remote electronic signature issues certificates to subscribers, who use and rely on the Penneo Platform through internet connection.

There are two types of subscribers for the remote electronic signature service:

1. **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.
2. **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 Signer Interaction Component before they sign.

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,

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- 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.

1.5. Policy administration

1.5.1. Organization administering the document

Penneo administers and manages this document.

1.5.2. Contact persons

The contact persons related to this document are:

- Information Security Manager - responsible for the policies governing the trust service
- Platform Manager - responsible for the technical operation of the trust service
- Product Manager - responsible for the functionality of the trust service

All questions and/or comments concerning this document shall be addressed to: trustservice@penneo.com

1.5.3. Person determining suitability for the policy

The persons determining the suitability of this document are:

- Platform Manager - responsible for the technical operation of the trust service
- Information Security Manager - responsible for the policies governing the trust service.

Results and recommendations from an eIDAS accredited auditor are considered by the responsible persons when determining the suitability of this document.

1.5.4. Approval procedures

The approval procedures and processes are managed by Penneo's managers. They determine employees performing the update, modification or changes based on these procedures.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

The final version of the performed update/modification is approved according to internal responsibilities by Penneo's managers.

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.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

	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

2.1. Repositories

Penneo operates repositories of private and public information and documentation.

Repositories are divided to:

- The public information presented via Penneo web pages;
- The part of internal documentation (for internal usage only);
- And the public repository implemented for issued certificates.

Public information includes:

- Certification Practice Statement;
- Certificate policies;
- Particular Practice Statements;
- Particular Disclosure statements;
- CAs and root CA certificates;

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- Lists of revoked certificates - Certificate Revocation List (CRL);
- Documents based on the applicable law.

2.2. Publication of certificate information

2.2.1. Published information

Address of Company: Gærtorvet 1-5, DK-1799 København V

Internet address: https://www.penneo.com

The publication of root CA certificates, subordinate CAs, certificates for electronic signature, seal and timestamps are available on the Penneo web pages and contain mainly:

- Certificate number;
- Name (contents from common name structure);
- Period of validity of the certificate;
- Object identifier of policy (OID policy);
- CRL address.

Certification policies, Practice statements, Disclosure statements and CPS can be viewed at:

https://eutl.penneo.com/

Certificate revocation list (CRL) contains information about:

- the date the CRL was issued;
- the CRL number;
- and the link where the CRL is available - included in a certificate.

The list of subscriber certificates are published in the public certificate repository. Details are described in particular CP.

Access to published information is realized via Internet protocols - HTTPS.

2.2.2. Unpublished information

Penneo reserves the right not to disclose information in accordance with internal security policies, procedures and processes.

2.3. Time or frequency of publication

Penneo issues public CA certificates and relevant Trust Service documents via designated public channels. See 2.1 and 2.2.

CA Certificates are published as soon as possible after they have been issued.

The frequency of issuing the CRL of the Root CA is minimum every 180 days, with a validity time of 180 days. Issued certificates are published immediately after approval of the root CA.

Current CP version is published immediately after approval including the version number.

Information about revoked certificates for some PKI services is published immediately.

2.4. Access controls on repositories

Public published information is accessible on Penneo's web pages in read only format. Access control prevents unauthorized access to modify, delete or add entries into repository.

3. Identification and authentication

3.1. Naming

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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

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

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 as the Subscriber they 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.

The RA/IP shall verify the subscriber identity and, if applicable, any specific attributes of the subscriber, a) by the physical presence of the subscriber on RA contact places; or b) using electronic identification methods that ensure the identification of the subscriber with a high level of confidence, the conformity of which has been confirmed by a conformity assessment body, or c) using electronic identification methods that are Notified as per eIDAS art. 9, with high level of assurance for qualified certificates, or with substantial level of assurance for non-qualified certificates.

RA/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 1.3.2.

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.

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- 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 signatures to natural persons. The Platform does not allow subscribers to obtain a certificate linked to a legal entity.

The Platform verifies that the customer is authorized to access the Platform based on their unique ID identifier when they log into the Platform to prepare documents for signature.

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 subscribers re-key process.

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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.

Certificate 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:

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.

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- 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

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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.

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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

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

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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

Services of Penneo's PKI are available for 7 days a week, 24 hours a day. 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

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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.

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

5.1. Physical security controls

5.1.1. Site location and constructions

Site location and constructions are physically protected and secured. The data centre center is strategically located to ensure they have power availability and connectivity.

Penneo's office space shall be secured through appropriate measures. Access to Penneo's office space shall not provide any direct access to internal or confidential information.

Office space does however present an asset that needs to be adequately protected for the access to PKI infrastructure, personal devices and rooms.

Applications are hosted in a cloud solution and used from an external vendor.

Penneo ensures that appropriate physical and environmental controls are in place around the devices issuing certificates.

Physical and environmental controls cover physical access control, perimeter security, natural disasters protection, fire safety, redundant power supply, disaster recovery and more.

5.1.2. Physical access

Penneo ensures that certificate issuing devices and other devices processing sensitive information are kept within secure areas that are protected by multiple appropriate entry barriers and security measures. This includes the following measures to secure the data centres:

- 24×7 security guards on site;
- Outer perimeter protection (fences, bollards, barriers);

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- Outer and inner perimeters surveillance cameras;
- Alarm system (sound and visual) and infrared sensors covering the whole perimeter (in and around the building), which are monitored 24×365 by security personnel;
- Physical access is restricted using mantraps, biometric controls and badge access regulated by role-based access;
- Access control system records any entries or exits in the building, private rooms and other private spaces.

5.1.3. Power and air conditioning

Penneo ensures that data centres hosting certificate issuing devices are equipped with sufficient air conditioning and power supply in order to provide suitable conditions for operating devices, as well as reliable and resilient power infrastructure. This includes dual energy access points to the facility, diesel generators with sufficient fuel storage, UPS systems and various redundant elements in the distribution network throughout the premises.

For optimum performance, equipment is maintained and continuously monitored in a climate-controlled environment. The average room temperature and humidity level is controlled at a suitable level. Multiple air conditioning units provide redundant capacity. Down-flow cooling units help ensure maximum cooling of equipment.

5.1.4. Water exposures

Penneo ensures that data center facilities include water detection systems installed in areas that may be susceptible to leakage. The water detection alarms are relayed directly to the service center, as well as to the relevant local security and engineering personnel.

5.1.5. Fire prevention and protection

Penneo ensures that data centre facilities are protected against damage from fire using fireproof doors and walls and fire suppression systems.

Temperature and smoke/fire alarms, optical smoke detectors (under the raised floor and on the ceiling), connected to main fire panel (dedicated per zone) and smoke detection system under floor and overhead and gaseous fire suppression system.

5.1.6. Media Storage

Penneo ensures that devices are handled in accordance to the instructions and protected against theft, damage and unauthorised access.

5.1.7. Waste Disposal

Penneo ensures that devices are disposed in a secure way and data is wiped in an appropriate way prior to disposal.

5.1.8. Off-Site Backup

Penneo ensures that a backup procedure is in place in order to restore services in case of system failure. Penneo stores backup material at two separate locations in order to ensure that certificate issuing devices can be can become operational in case of a disruption. Other components operated from Penneo's cloud infrastructure are backed up at a second region.

5.2. Procedural controls

5.2.1. Trusted roles

Penneo has defined trusted roles to ensure that persons involved in the operations related to certificate issuing devices do so in a trusted capacity. Trusted roles are defined to prevent conflict of interests and that Penneo's trusted service does not rely on a single person or that one person can single handedly operate the system.

The following trusted roles have been defined:

- Security Managers
- System Administrators
- System Operators

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- System Auditors

5.2.2. Number of persons required per task

Penneo has implemented internal procedures and controls to ensure that no single trusted person shall be able to perform critical tasks alone. Critical tasks include CA key pair generation and generating a CRL.

5.2.3. Identification and authentication for each role

Penneo ensures that persons go through Penneo's hiring process to ensure the suitability and that the person possesses the required qualifications for a given role. Before a person is granted access to certificate generating systems, the person must be formally appointed to a trusted role by the Security Manager.

The authentication to Penneo's trusted systems follows internal procedures and controls.

5.2.4. Roles requiring separation of duties

Penneo applies the need to know and least privilege principles to allocate access rights to users. Certificate generating services and other highly sensitive systems have dual control to ensure that no person can perform changes without the involvement of another trusted person.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

Penneo has defined and implemented a process for hiring that must be followed. The process ensures that the person is identified and fulfills the requirements needed to fill a certain role. Before access is granted to Penneo's trust service, a person must be formally appointed.

5.3.2. Background check procedures

Penneo only appoints personnel who are considered trustworthy to a trusted role. A person must have been through Penneo's hiring process and a check of a persons criminal record must have been performed. When being appointed to a trusted role, the person must acknowledge the responsibility that comes with the trusted role and what requirements apply to the trust service.

5.3.3. Training requirements

Penneo ensures that all new employees complete an onboarding awareness training.

Penneo shall provide persons involved in the development, operations and maintenance of Penneo's trusted service with relevant training based on a trusted person's needs.

5.3.4. Retraining frequency and sequence

Areas that require a certain basic level of awareness on a continuous basis shall be updated at least annually.

As a minimum, all employees shall complete an annual update concerning Security, Compliance, and GDPR.

Trusted persons shall make sure they maintain skill levels necessary to fulfill the tasks related to the trusted role to which they have been appointed.

5.3.5. Job rotation frequency and sequence

Penneo shall ensure that the trust service operations are not affected by personnel changes within Penneo.

5.3.6. Sanctions for unauthorized actions

Penneo will evaluate violations of applicable policies and procedures on a case-by-case basis. Penneo's management will determine appropriate disciplinary actions where necessary.

5.3.7. Independent contractor requirements

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Penneo does not engage independent contractors to operate its trust service components. Penneo may engage independent contractors to perform work related to the trust service. Penneo will at all times maintain the control and oversight of the trusted service.

5.3.8. Documentation supplied to personnel

All new employees go through an onboarding process when joining Penneo. During the onboarding the new Penneo is introduced to the organisation, Penneo's values, code of conduct and applicable policies, standards and legislation.

All existing Penneo employees must complete an annual awareness training that includes elements related to information security and data privacy.

5.4. Audit logging procedures

Penneo ensures that relevant activities concerning the operations of the trust service are captured via related audit logs. The integrity, availability and confidentiality of the data transmitted and stored are maintained during the collection of audit data to audit logs.

The audit system:

- ensures the maintenance of audit data and the provision of sufficient space for audit data;
- the automatic non-rewriting of the audit file;
- the presentation of audit records to users in a suitable manner;
- the limited access to audit file for responsible employee only.

5.4.1. Types of events recorded

A set up for creating and storing audit/event logs shall be in place for relevant logs. The setup shall ensure that audit/event logs related to the CAs are collected.

With regard to the requirements of relevant technical standards and the law specified for trust-building services, the trusted Penneo's systems record:

- significant events in the Penneo's environment and keys processing;
- start and end of audit functions, changes in audit parameters;
- all attempts to access the system;
- all events related to the certificate life-cycle;
- events about person's access and registration;
- events about an attempted unauthorized access;
- events related to the subscribers certificate life cycle:
    - events about the issuance of the certificate, including the result;
    - about the unjustified request for the issuance of the Certificate, including the result;
    - the request for revocation of the certificate, including data of employees or subscribers;
    - the unjustified request for revocation of the certificate, including data about the person and the result;
    - about the publication of the certificate, including the result;
    - revocation and publishing to CRL.

Records in the audit file contain:

- date (year, month, day) and time (hour, minute, second) of the event,
- type of event,
- identity of the employee/subscribers that is performing for the action,
- success or failure of event.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

5.4.2. Frequency of processing log

Logs shall be regularly reviewed for the purpose of detecting suspicious activities.

5.4.3. Retention period for audit log

Audit logs records shall be kept for at least 7 years from the date of their creation.

Other event logs will not considered audit logs shall be retained based on internal requirements.

Audit logs will be made available to accredited Auditors upon request.

5.4.4. Protection of audit log

The audit system is created and operated on the environment with sufficient capacity, without the possibility to use common access to stored data.

Logs are sent to a dedicated log server and logs cannot be edited or deleted by any user.

5.4.5. Audit log backup procedures

Audit logs shall be securely stored and backups created.

Copies of logs are transferred to a safe environment and access is regulated to responsible persons only.

The steps for audit logs backup procedures are the same as during backups of others electronic information.

5.4.6. Audit collection system (internal vs. external)

Audit log collection system is operated by Penneo and does not depend on external sources.

5.4.7. Notification to event-causing subject

No one who caused the incident is informed.

5.4.8. Vulnerability assessment

Penneo shall perform a risk assessment at least on an annual basis. Risk assessments shall follow the methodology as defined by the ISO 27005 standard.

Penneo shall perform vulnerability scans and penetration testing covering the trusted services including CAs.

The tests shall focus on internal and external threats towards the trust service and the information processes therein.

5.5. Records archival

Penneo shall archive records to establish the events that have taken place in relation to the issuance or certificates.

5.5.1. Types of records archived

Penneo archives especially:

- records from Root CA and subordinate CA's initialization;
- signed protocol from initializations ceremony;
- audit reports;
- evaluation of Penneo based on legal and law requirements;
- information from business contracts, initialization, cancellation, content of contracts;
- particular version of Platform programs;
- product and technical documentation, application software, version of applications and documents.

5.5.2. Retention period for archive

Root CA records and subordinates CA records are archived for the all time of PKI trust services which Penneo uses for business activities.

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Audit logs are archived minimally for 7 years.

5.5.3. Protection of archive

Archive records are protected against modifications.

5.5.4 Archive backup procedures

Archive records are protected based on technical and object security. Inside internal documentation are described requirements for protection of archive records.

5.5.5 Requirements for time-stamping of records

In the cases of time stamp usage, Penneo uses electronic qualified time stamps for subscribers.

5.5.6 Archive collection system (internal or external)

Penneo uses system based on cooperation with external suppliers. The place is managed by responsible manager of Penneo.

5.5.6 Archive collection system (internal or external)

Penneo is responsible for the archiving of relevant logs and documentation. Penneo uses appropriate tools provided by external vendors.

5.5.7 Procedures to obtain and verify archive information

The information is kept and is located in the locations designated for this purpose and is accessible to:

- Penneo's employees, if required for their activities,
- authorized supervisory and control bodies and bodies active in criminal matters, if it is required by other standards.

5.6 Key changeover

Penneo distinguishes between several types of actions:

- common change of root CA keys - before expiration of valid certificate, minimally a year in advance has to be new ceremony of keys generation and issuing of the new root CA certificate (self-signed certificate).
- common change of subordinates CA keys - before expiration of valid certificate, minimally a year in advance has to be sent new certification application for subordinates CA;
- common keys change of electronic seal and time stamp certificate - before expiration of common and valid certificate - minimally 1 year before, is issued the new key pair and the new certificate;
- after suspicion of abuse of the private key - immediately after suspicion, is issued the new key pair and the new certificate,
- after possible technical problems - based on:
    - lower security of cryptographic algorithms,
    - length of keys,
    - new methods and improving of security,

is issued the new key pair and new certificate.

Upon expiration of CAs certificates the old ones has to be deleted and written protocol created. The back up and cryptographic environment has to be initialized.

Information about changes of CAs certificates has to published on Penneo's web pages in advance.

5.7. Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Penneo established business continuity procedures and disaster recovery plans, which includes:

- procedures that solve incidents and compromise problems;
- business continuity management and disaster recovery policy;
- risk management policy.

Risk management is performed regularly and must be performed at least on an annual basis but should be updated whenever new relevant threats and vulnerabilities are identified. Hence, the risk management process is continuous.

The risk identification shall only take relevant risks into account. Risks considered negligible due to an extremely low probability of occurrence or extremely low potential impact will not be included for further analysis in as part of the risk assessment.

Special internal procedures addresses problems with:

- misusing of CA private key. Immediately actions have to be performed, as described in internal procedures;
- lost of necessary and needed data or misuse of private information;
- breach of security with impact on business of Penneo's;
- lost of documentation and detailed description of processes;
- breach of Penneo Platform or outages of used SW and HW.

Analysis and recovery processes have to be started.

5.7.2 Computing resources, software, and/or data are corrupted

Corruption of computing resources, software and data security are managed by internal procedures and resources. Service level agreements are concluded to agreement with suppliers.

5.7.3 Entity private key compromise procedures

In the case a root CA private key is compromised Penneo will:

- disconnect usage of automated Platform and cooperating PKI services for remote electronic signature, seal and time-stamp;
- revocation of the root CA certificate;
- revocation of subordinates CA certificates;
- revocation of all valid certificates issued by those CAs.

Immediately publish information on Penneo's web pages and revoked certificates are published in relating CRLs. Information about revocation activities has to be sent to all subscribers (based on agreements between Penneo's and subscribers).

All private key (including seal private key) and back-ups will be deleted and secure encryption environment initialised. About initialisation and private key destroying is written protocol signed and published.

In the case a subordinate CA private key is compromised Penneo will:

- immediately stop usage of the particular CA certificates and disconnect usage of automated Platform and cooperating particular CA service;
- revocation of the particular CA certificate by the Root CA and issuing of the new CRL;
- all subscribers will be informed about private key compromising and will be notified of the particular CA termination;
- revocation of all certificates issued by the particular CA and issuing of the new CRL.

The particular CA private key and back-ups will be deleted and secure encryption environment initialized. About initialization and private key destroying is written protocol signed and published.

5.7.3.3. Subscriber private key compromising

In the case of the private key compromising Penneo performs following steps:

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- immediately stop an usage of the certificate;
- immediately disconnect usage of automated process for remote electronic signature (the Platform);
- immediately inform subscribers about situation - Penneo's web pages, Penneo's server and third parties (if they cooperates) - that the Platform is stopped and problems analyzed;
- make steps to recover all process as fast as possible and start the Platform.

5.7.5 Business continuity capabilities after a disaster

Penneo uses hosting providers that have necessary measures in place to deal with unexpected events. Penneo manages business continuity capabilities and has internal procedures for reacting to different scenarios.

5.8 CA or RA termination

5.8.1. CA termination

The Qualified Trust Service provided by Penneo is a significant asset to the company. This means that any significant changes will be discussed at executive and board level. I.e.

Penneo has a Termination Policy that has been signed by the CEO. This ensures that the CEO is aware of the requirements related to any termination of Qualified Trust Service by Penneo and that this must be communicated to subscribers.

Penneo has a documented process for company announcements and guidelines for information that is considered insider information and therefore must be announced to the market.

The termination policy will take effect if management decides to either terminate trust service operations in whole or in part or transfer the ownership of the operations to a third party in whole or in part, the following steps must taken and detailed plans must be prepared to ensure successful execution.

Termination of the trusted service in its entirety or in part (e.g. only time stamp issuing but not remote signing) can be realized through one of the following options:

Penneo's management decides to cease operations of the trusted service as a whole or in part.

Penneo will keep operating the domain and Certificate Revocation List (CRL) to ensure continuous validation of existing signatures, timestamps and certificate issuing despite the service as a whole or in part being terminated.

Penneo must cease operation of trusted service and has no possibility to keep operating the domain and CRL to ensure continuous validation of existing signatures.

a CRL must be issued with the same validity as the Certificate Authority (CA) in order to verify existing signatures;

the operations including CA and CRL are handed over to the supervisory body or another reliable party which will ensure continuous validation of existing signatures.

Trusted service is transferred to another certified TSP.

In case management decides on a new strategic direction, which leads to either Penneo choosing to terminate/cease operations or transferring the ownership of the operations to a third party, the following steps must taken and detailed plans is prepared to ensure successful execution:

- preparation phase
- execution phase
- communication phase

Every information is backed up and accessible to all clients and legal companies for possible securing evidence.

Penneo ensures the all operation for the necessary period - availability of CRL, CP, PS and CPS for issued certificates and time period is minimal to the last valid of issued certificates.

The process of CA or PKI services termination is managed based on internal documentation and internal plans: Termination Policy (for QTS).

All private keys have to be deleted and the secure cryptographic module initialized.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

5.8.2. RA termination

Process of RA termination is described within internal RA/IP documentation and the agreement between Penneo company and companies performing activities in roles of identity providers/Registration authorities.

TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Subscribers private keys are generated and saved to cryptographic module and used directly by the automated Platform processes for remote qualified electronic signature, seal and time stamp.

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.

6.1.5 Key sizes

Key size of root CA is 4096 bits (RSA algorithm).

Key size of subordinate CA and TSA certificates is 4096 bits (RSA algorithm).

Key size of subscribers certificates is 3072 bits or higher (RSA algorithm).

6.1.6 Public key parameters generation and quality checking

Parameters of keys are relevant to legal requests for eIDAS or EU and standards. Key pairs are generated based on the supplier’s delivered software and hardware generation tool and use mechanisms from the secure cryptographic modules.

Parameters for subscribers are defined in advance and implemented to the hardware security module which is responsible for the key pair generation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usage purposes are defined in the certificate extension.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

All private keys are saved in cryptographic hardware security modules owned and controlled by Penneo.

Subscribers’ keys can only be activated through the Platform’s automated services to customers and signers. The hardware security modules are integrated in the Platform according to technical standards.

6.2.1 Cryptographic module standards and controls

Standard for root CA cryptographic hardware security module is Common Criteria EAL 5 (CC-18-98209). A trusted channel and public key attestation allow remote key generation and certificate issuance. Advanced key management functions provide for key backup and escrow.

Generation of remote key pairs for subordinate CAs (for remote electronic signature, seal and time stamps) are performed in the hardware security modules which are certified by Common Criteria as well (Common criteria level 4+).

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Before initialisation procedure Penneo verifies if all hardware security modules are sent in the original packaging and delivery is without complication or problems.

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

The subscriber’s private key is available to the subscriber during remote and automated remote signing process only.

6.2.3 Private key escrow

The service of private key escrow is not provided for subscribers.

6.2.4 Private key backup

The cryptographic module supports encrypted key backup and restore using mechanisms that can be set during cryptographic modules initialization.

Subscribers private key is not 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. The electronic signature performed inside hardware cryptographic module and there is no reason to transfer the private key from the cryptographic module.

6.2.7 Private key storage on cryptographic module

Private keys of Penneo’s PKI Services in unencrypted state are stored in activated and initialized hardware security modules that meet the requirements of the legislation for qualified trust services.

For cryptographic module activation and initialization minimally two authorized Penneo employees have to cooperate.

The subscriber's private key for electronic signature certificates is stored in the cryptographic hardware security module and deleted after the signature has been created. If the subscriber needs to complete multiple signing processes, separate keys and certificates will be issued each tie, subject to the subscriber's repeated identification and acceptance.

6.2.8 Method of activating private key

The subscriber's private signing key is activated by the Penneo Platform on their behalf during the automated remote signing process.

The private keys of Penneo's TSA certificate and seal certificate are activated by the Penneo Platform through the Platform's automated process, subject to authorisation as described in internal documentation.

Activation of private keys of the CAs certificates is performed with the direct personal participation of at least two Penneo’s responsible persons authorized by Penneo’s management. Such activation is performed according to a precisely determined procedures and tools managed by Penneo, which are regulated by internal documentation.

A written protocol is created based on performed activities.

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.

6.2.11 Cryptographic Module Rating

Penneo uses cryptographic hardware security modules (HSMs) for key pairs generation and storage of CAs private keys. The HSMs meet the requirements of the legislation for qualified trust services (The Common Criteria EAL 5 and 4+).

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

The HSMs are integrated in Penneo's Platform and are certified for qualified remote electronic signature, seal and time stamp. The implementation and security is regularly monitored and checked.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Penneo archives all issued certificates.

Retention period is a minimum of 7 years.

6.3.2 Certificate operational periods and key pair usage periods

Subscriber certificate operational period is defined in the certificate.

Certificates for Penneo's PKI services are issued for time specified in the particular certificate. The operational period may end by revocation request. Penneo's trust certificates are not used beyond end of validity.

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

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data for qualified remote electronic signature is generated within the Platform during a particular session. It is sent 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.

The Platform maintains the signing session, thereby ensuring that the key is always linked to the subscriber, and to the given SAD, DTBS and SAP.

Activation data fulfils requirements of implemented and initialised hardware security module (data length, data composition, data distribution).

6.4.2 Activation data protection

Activation data is handled within the Platform through secure network connections. Protection of the relevant Platform components and network is described in internal documentation.

6.4.3 Other aspects of activation data

Activation data of CAs must not be transmitted or kept in an open form.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The strategic goal of Penneo is to make information security as the integral part of the company culture.

The key strategic goals for the Penneo's business:

- Keep subscriber's data confidential and safe;
- Deliver signed documents with the following verifiable properties:
    - The identity of the signer(s) can be uniquely established (Authenticity);
    - The signer(s) cannot deny having signed the document (non-repudiation);
    - The document can not be modified undetected (Integrity).
- Keep product reliability and availability as close to 100% as possible.

Penneo shall implement necessary technical and organizational security measures against sensitive data being accidentally or unlawfully destroyed, lost or impaired and against any unauthorized persons receiving the personal data, the personal data being abused or otherwise processed contrary to the legislation.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

6.5.2 Computer security rating

- Family ITU-T
  - 501, X.509, X.520
- RFC
  - 2560, 3647, 5280, 6962
- ISO/IEC
  - 17021, 17065, 3166-1
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements.
- CEN/TS 419 261 Security requirements for trustworthy systems managing certificates and time-stamps.
- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA),

6.6 Life cycle technical controls

6.6.1 System development controls

Penneo's software is built from the ground up to be easy and painless to deploy and maintain.

Hardware used to operate to issue certificates are from trusted sources and checked and used according to manufacturing specifications.

All releases are done according to Penneo's software development policy, which includes testing and reviews prior to release.

6.6.2 Security management controls

Verification of controls is performed regularly base on ISO/IEC 2700X principles and standards. In order to ensure compliance to policies and working instructions as defined within this ISMS continuous monitoring and auditing shall be implemented and tracked. The responsibility for the monitoring and auditing lies with the Information Security Manager who is the head of the Risk & Compliance department.

6.6.3 Life cycle security controls

Penneo uses during the all phases of development and implementation independent life-cycle security controls defined in internal documentation /and others standards.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Penneo performs clearly defined process for development of software from the storage and management of source code to deployment of releases and hot fixes.

6.7 Network security controls

Penneo uses layered security of its networks that operate the trust service.

Network segmentation is implemented to ensure that Penneo's applications are logically separated and no access to other resources is permitted.

Penneo's production environment is not directly accessible from the internet.

Penneo's root CA is off-line. It is not connected to a network.

6.8 Time-stamping

Time-stamping is used during remote electronic signature and seal and the all data is verified and transferred by secure channel.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificates issued according to this CP are in accordance with the standard ISO 9594-8 (X.509) and RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Basic certificate fields:

#	Field	Sub-fields in SEQUENCE	Description	Mandatory / Optional / Critical	Value
1	version		Version of the certificate that complies with with X.509 standard, version 3.	MANDATORY	v3 (0x2)
2	serialNumber		Unique serial number of the certificate assigned by the CA.	MANDATORY	Positive integer explicitly assigned by the CA
3	signatureAlgorithm		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	MANDATORY	**sha512withRSAandMGF1**
4	issuer		Distinguished Name of the Issuer's certificate.	MANDATORY	X.509 type Name
5	validity				ASN.1 SEQUENCE
6		notBefore	The date on which the certificate validity period begins	MANDATORY	UTCTime
7		notAfter	The date on which the certificate validity period ends.	MANDATORY	notBefore + 1 day
8	subject		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See Subject Field below for details.	MANDATORY	X.509 type Name
9	subjectPublicKeyInfo				ASN.1 SEQUENCE

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

#	Field	Sub-fields in SEQUENCE	Description	Mandatory / Optional / Critical	Value
10		algorithm	Identifies the algorithm with which the key is used.	MANDATORY	**sha512withRSAandMGF1**
11		subjectPublicKey	Public key of the associated entity.	MANDATORY	minimum 3072 bits for RSA keys
12	extensions		Sequence of one or more certificate extensions. See Certificate Extenstions below for details.	MANDATORY	ASN.1 SEQUENCE
13	signatureValue		Qualified electronic seal of the trust service provider Intermediate CA.	MANDATORY	Signature represented as BIT STRING

Issuer Field

Issuer of the certificate for electronic signature is Penneo's Intermediate Qualified CA. **Subject Field**

#	Item	Description	Mandatory / Optional / Critical	Comments
1	countryName	Country code.	MANDATORY	Two characters based on ISO 3166 DK for Denmark
2	givenName	Subscriber's first name.	MANDATORY	
3	surname	Subscriber's surname.	MANDATORY	
4	commonName	Identification of the subscriber within the CA.	MANDATORY	
5	organisationName	Organisation name where the subscriber is employed or which is represented by the subscriber.	OPTIONAL	Name of the organisation based on the Business Register
6	organisationIdentifier	Identification number of the organisation.	OPTIONAL MANDATORY if the **organisationName** is present	id-etsi-qcs-SemanticsId-Legal semantics
7	serialNumber	Identification of the subscriber.	MANDATORY	id-etsi-qcs-SemanticsId-Natural semantics
8	title	Designated position or function of the subject within the organization specified.	OPTIONAL	String

7.1.1 Version number(s)

The certificate issued according to this CP complies with the ISO 9594-8 (X.509) standard, version 3. The certification services provided by KB do not support certificates of another type or other versions of the X.509 certificate.

7.1.2 Certificate extensions

#	Extension	Description	Content	Mandatory / Optional / Critical	Comments
1	AuthorityKeyIdentifier			NOT CRITICAL MANDATORY	Two characters based on IS

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

2		keyIdentifier	Identification of the public key corresponding to the private key used to sign a certificate.		160 bit SHA-1/SHA-512 hasl the value of the public key c CA certificate
3	SubjectKeyIdentifier		Identification of certificates that contain a the subject public key.	NOT CRITICAL MANDATORY	160 bit SHA-1/SHA-512 hasl the value of the public key c subscriber's certificate
4	KeyUsage		Defines the purpose of the key contained in the certificate.	CRITICAL MANDATORY	digitalSignature nonRepudia
5	CertificatePolicies		Sequence of one or more policy information terms according to which was certificate issued.	NOT CRITICAL MANDATORY	
6	PolicyInformation [1]	policyIdentifier	Identification of the policy.		OID of the certificate policy
7		policyQualifiers	Pointer to a Certification Practice Statement (CPS) published by the CA.		cPSuri: http... userNotice: T certificate for the electronic issued in accordance with F No 910/2014. This is a quali for electronic signature acc Regulation (EU) No 910/201
8	PolicyInformation [2]	policyIdentifier	Identification of the policy.		QCP-n-qscd 0.4.0.194112.1.:
9	SubjectAlternativeName			NOT CRITICAL	
10		rfc822Name	E-mail address of the subscriber.	OPTIONAL	Valid e-mail address
11		uniformResourceIdentifier	Transaction ID	OPTIONAL	Identification of the transac
12		uniformResourceIdentifier	SAM key ID	OPTIONAL	Identification of the remote
13	BasicConstraints		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.	CRITICAL MANDATORY	
14		cA	Identifies whether the		FALSE

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

			subject of the certificate is a CA.		
15	ExtendedKeyUsage		Indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.	NOT CRITICAL MANDATORY	• MS Document Signing:1.3.6.1.4.1.311.10.3.12 Authentic Documents Trust 1.2.840.113583.1.1.5
16	CRLDistributionPoints		Identifies how CRL information is obtained.	NOT CRITICAL MANDATORY	URI https://crl.prod.qs.penneo.c of the CA issuing CRL>/<Id
17	AuthorityInformationAccess		Indicates how to access information and services for the issuer of the certificate.	NOT CRITICAL MANDATORY	
18		id-ad-calssuers	Access CA certificate.		URI https://ca.prod.qs.penneo.c of the CA>/<Id of the CA>.c
19		id-ad-ocsp	Access CA OCSP service.		URI
20	QCStatements*			NOT CRITICAL MANDATORY	
21		id-etsi-qcs-QcCompliance	QCStatement claiming that the certificate is a EU qualified certificate or a certificate being qualified within a defined legal framework from an identified country or set of countries.		0.4.0.1862.1.1
22		id-etsi-qcs-QcSSCD	QCStatement claiming that the private key related to the certified public key resides in a QSCD.		0.4.0.1862.1.4
23		id-etsi-qcs-QcType	QCStatement claiming that the certificate		id-etsi-qct-esign

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

			is a certificate of a particular type.		
24		id-etsi-qcs-QcPDS	QCStatement regarding location of PKI Disclosure Statements (PDS).		URL and language 0.4.0.186

*Included for all Qualified Certificates. Omitted when certificates are issued for Advanced Electronic Signature.

7.1.3 Algorithm object identifiers

Algorithm is defined in related technical standards.

7.1.4 Name forms

Name forms correspond to identification of subscriber and ID structure issued by registration authorities.

7.1.5 Name constraints

The item “CN” does not contain a domain name.

7.1.6 Certificate policy object identifier

OID of this CP is defined based on related technical standards and used in subscriber’s certificate.

7.1.7 Usage of Policy Constraints extension

It is not relevant to this policy.

7.1.8 Policy qualifiers syntax and semantics

See chapter 7.1.2.

7.1.9 Processing semantics for the critical Certificate Policies extension

See chapter 7.1.2.

7.2 CRL profile

Penneo supports CRL version 2, available through certificate register according to standard DAP (LDAP).

As a alternative to CRL in LDAP Penneo can use a WEB services or others services passing for certificates verification. Revocation status information is available beyond the validity period of the certificate. Revoked certificates after they have expired are not in the CRL.

#	Field	Sub-fields in SEQUENCE	Description	Value
1	version		Version of the certificate that complies with with X.509 standard, version 3.	v2 (0x1)
2	signatureAlgorithm		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	minimum SHA256WithRSAEncryption (1.2.840.113549.1.1.11)
3	issuer		Distinguished Name of the Issuer’s certificate.	X.509 type Name
4	thisUpdate		Issue date of the CRL	UTCTime
5	nextUpdate		The date by which the next CRL will be issued.	UTCTime
6	revokedCertificates		List of revoked certificates.	

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

#	Field	Sub-fields in SEQUENCE	Description	Value
7		userCertificate	Serial number of revoked certificate.	CertificateSerialNumber
8		revocationDate	Time when the certificate was revoked.	UTCTime
9		crlEntryExtensions	Sequence of one or more certificate revocation list extensions. See CRL Extenstions below for details.	ASN.1 SEQUENCE
10	crlExtensions		Sequence of one or more certificate revocation list extensions. See CRL Extenstions below for details.	ASN.1 SEQUENCE
11	signatureValue		Qualified electronic seal of the trust service provider Intermediate CA.	Signature represented as BIT STRING

7.2.1 Version number(s)

Penneo's Services use a CRL according to the PKIX profile (RFC 2459), which is an implementation of the X.509v2 list, defined by the ISO / IEC / ITU specification from 1997.

7.2.2 CRL and CRL entry extensions

#	Extension	Sub-fields in SEQUENCE	Description	Content
1	crlReason		Reason of the revocation.	unspecified (0) keyCompromise (1) cACompromise (2) affiliationChanged (3) superseded (4) cessationOfOperation (5) certificateHold (6) removeFromCRL (8) privilegeWithdrawn (9) aACompromise (10)
2	AuthorityKeyIdentifier			
3		keyIdentifier	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1/SHA-512 hash function on the value of the public key of the signing CA certificate
4	crlNumber		Unique number of the CRL.	Value up to 20 octets

7.3 OCSP profile

OCSP protocol is not used.

8. Compliance Audit and other Assessments

To ensure that Penneo's subscribers can trust Penneo and Penneo's Trust Service is audited by an accredited conformity assessment body (Auditor) against the eIDAS regulation and applicable standards.

Penneo's trusted services require implementation of corresponding legislation, standards and procedures to fulfil eIDAS regulation.

Penneo completes ISO 27001 and 27701 certification audits on an annual basis to ensure appropriate internal controls are implemented and effective.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

8.1 Frequency or circumstances of assessment

Compliance to eIDAS requirements is audited every two years by the accredited Auditor.

ISO 27001 and 27701 audits of internal processes and controls are completed every year by a Certified Public Accountant with Information Security expertise.

Subject to due identification and signing of a non disclosure declaration, Penneo is obliged to allow access to its physical facilitates to authorities, or representatives acting on behalf of an authority, who in accordance with the legislation in force at any time have right to access the facilities.

Penneo also performs internal audits.

8.2 Identity/qualifications of assessor

Penneo's Trust Service must be audited by an accredited Auditor. The accredited Auditor must be trained for auditing such services and be independent of the audit subject. The accredited Auditor must be free from conflicts of interest.

Other auditors must be independent of Penneo and able to demonstrate the required expertise and experience in performing audit activities.

8.3 Assessor's relationship to assessed entity

External audits must be performed by a person/legal entity independent of Penneo.

Internal audits are performed by Penneo employees.

8.4 Topics covered by assessment

Audits must be completed in accordance to the standards applicable for the given audit and meet the requirements of the audit scheme applicable to the defined scope.

8.5 Actions taken as a result of deficiency

Should any deficiencies be identified through any audit activities, appropriate risk treatments must be initiated to remediate the deficiency.

The risk treatment plan is managed as part of the risk management process.

8.6 Communication of results

Results of audits must be reported to Penneo's Information Security Manager in writing for analysis. Deficiencies will be deal with as specified under 8.5.

Audit results will be shared with relevant stakeholders.

9. Other Business and Legal Matters

9.1 Fees

Fees are determined on a case by case basis to match the need of a person or organisation.

It is necessary to differ between a price list of identity provider functioning as registration authority and Services of Penneo.

In the case of cooperation agreement between Penneo and the Customers, fees can be defined in an attachment of the agreement.

9.1.1 Certificate issuance or renewal fees

Penneo issues Certificates as part of its Trust Service and may charge a fee for either issuance of Certificates or Subscription for use of service.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Applicable fees will be stated in the Terms of the contract between Penneo and Customer. The fees paid by the Customer covers certificate issuance, time stamping and sealing for all the Customer's Signers and documents.

9.1.2 Certificate access fees

Subscribers' certificates are used in fully automated processes within the Platform. Since certificates are not accessed separately by subscribers, only the certificate issuance fee applies.

9.1.3 Revocation or status information access fees

Revocation or status information access is free of charge.

9.1.4 Fees for other services

Fees for other services are defined in customers' Agreement.

9.1.5 Refund policy

It is not relevant for this document.

9.2 Financial responsibility

Penneo actively manages its finances through regular budget rounds to ensure sufficient resources to maintain operations and further develop the trust service. Since the beginning of 2025 Penneo is no longer a listed company but operates as a wholly owned subsidiary of Visma AS. Through this ownership structure, Penneo has access to Visma's cash pool. Visma is one of the world's leading software companies, owned by HG Capital, which provides Penneo with a strong and stable financial foundation.

9.2.1 Insurance coverage

Penneo has insurance coverage of its civil liability, with an insurance of professional civil liability that complies with the current regulation applicable and to maintain the customary and sound insurance level, including as a minimum product liability insurance and general liability insurance to cover Penneo's liability in accordance with our customer agreements. In addition to this, Penneo is liable for product liability in accordance with the general rules of damages of Danish law. Penneo's liability for damages in each case, is limited to the amount which is paid out in accordance with Penneo's product liability insurance in force at any time.

Penneo declares that it has valid business risk insurance in such a way as to cover possible financial damages.

Penneo has arranged liability insurance for all employees for damages caused by the employer to the extent determined by the Danish Employment Insurance Law and the insurance company.

9.2.2 Other insurance and assets

Penneo declares that it has sufficient financial resources and other financial security for the provision of the Services with regard to the risk of liability for damage.

Detailed information on the assets of Penneo can be obtained from the Annual Report of Penneo published in the Commercial Register.

9.2.3 Insurance or warranty coverage for end-entities

Penneo does not provide this service.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential information is everything that is not accessible on web pages of Penneo or available on print papers or governed by a contract between Penneo and subscribers.

Sensitive and confidential information include:

- private keys

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- internal documents, rules and procedures
- personal data:
  - In order for the Platform to function in accordance with the Agreement the following personal data will be processed each time:
    - Name,
    - IP-address,
    - e-mail address,
    - Electronic ID informations, and
    - social security number, if this is chosen by the Data Controller for each document send for signing to a third party.
- Penneo's business information;
- Subscriber's business information.

Internal and confidential documents can be shared with external parties if an non-disclosure agreement (NDA) has been signed by wither the individually or with the company engaged by Penneo.

9.3.2 Information not within the scope of confidential information

Information outside of scope of confidential information are marked as Public and are available on contact places of Penneo.

9.3.3 Responsibility to protect confidential information

Every employee in the Penneo has a duty to maintain confidential information. It is exactly defined in internal documents.

9.4 Privacy of personal information

9.4.1 Privacy plan

Penneo ensures the protection of personal data for subscribers to whom Penneo provides PKI trust services.

9.4.2 Information treated as private

Penneo provides personal information based on contract between Penneo and subscribers (regulated by the certification policies to subscribers, relying parties, as well as external auditors) for the purpose of a compliance audits, and for legal point of view in cases of criminal activities.

The Data Protection Officer is responsible for ensuring that operational processes within Penneo are in compliance to GDPR.

9.4.3 Information not deemed private

Information not deemed private is everything what is not marked as a private and content is not under protection based on legal acts.

A Data Privacy Statement outlining how Penneo handles personally identifiable information (PII) shall be written and made available to external stakeholders.

9.4.4 Responsibility to protect private information

The Data Protection Officer is responsible for ensuring that operational processes within Penneo are compliant to GDPR.

9.4.5 Notice and consent to use private information

The process is managed by legal acts and regulation. Data Processing Agreement (DPA), which forms part of the contract between Penneo and each respective customer, shall be available. The DPA shall be available on Penneo's website.

9.4.6 Disclosure pursuant to judicial or administrative process

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Compliance in regards to the EU regulation General Data Protection Regulation 2016/679 (GDPR). All processed information is accessible to authorities entitled by law in case when it is legally required.

9.4.7 Other information disclosure circumstances

All Penneo's employees shall ensure that his/her behaviour does not result in violations to the privacy of subscribers of Penneo and shall report any incidents including incidents involving PII.

9.5 Intellectual property rights

The Certificate Practice Statement, Certificate Policy, particular Practice Statements and other related documents are protected by the copyright of Penneo company and represent its significant know-how.

Penneo is also owner and holder of rights to the web based application (the structure, the content and particular steps) fulfilling procedures of the certification authorities and trust services for electronic signature, time-stamp and electronic seal.

Penneo has intellectual property rights on issued certificates and used exclusively for electronic signature, time-stamp and seal. Key pairs are the property of the subscribers (legal or natural).

Penneo has a European trademark to the word Penneo, in relation to the function and services the Penneo Sign product provides.

9.6 Representations and warranties

Penneo guarantees that all requirements are met concerning, certificate policies and CPS, and internal documents and procedures.

9.6.1 CA representations and warranties

Penneo manages all PKI trust services and provides qualified services in accordance with:

- relevant certification policy;
- certificate practices statement;
- relevant Practice statement,
- PKI, TSA disclosure agreement,
- internal operational documentation,
- applicable national and EU legislation and legal acts.

9.6.1.1. Penneo's Qualified Root CA

Penneo's Root Certification Authority guarantees:

- that use CA's private keys only for issuing certificates to subordinate CAs;
- that issues a certificate conforming to the X.509 standard, internal documentation and procedures;
- that publishes the CP on Penneo's web pages;
- that publishes Root CA's certificate on Penneo's web pages;
- that publishes CRLs regularly on Penneo's web pages;
- in the case of Root CA's certificate revocation informs subscribers and relying parties and publishes information about the certificate revocation.

9.6.1.2. Penneo's qualified Subordinate CA for electronic signature and time-stamp.

Penneo's qualified subordinates CAs (for electronic signature and time-stamp) guarantees:

- that certificates issued to subscribers and for theirs needs meet the requirements required by the legislation for trust services and the relevant technical standards and norms

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

- publish the certification policies under which it issues certificates on its website
- in the case of Subordinate CA's certificate revocation informs subscribers and relying parties and publishes information about the certificate revocation;
- The Platform and technical infrastructure are in accordance with EU technical standards and EU legislative;
- that all needed information about issued certificates, CRL, CP, Practice Statements and CPS are available on the Penneo's web pages.

All guarantees can be managed and fulfilled if the certificate holder and relying parties fulfil all conditions and obligations concerning to the CP and contract between Penneo and subscribers.

9.6.2 RA representations and warranties

The relation between Penneo and registration authorities (identity providers) are managed via agreement. Registration authorities fulfil their own business model which guarantees that the identity of subscribers is verified and valid based on related legal conditions.

9.6.3 Subscriber representations and warranties

All information about representation and warranties are included to the agreement between Penneo and the subscriber.

Penneo rejects any other guarantee that is not enforceable under the laws, except the ones covered in section 9.6.2

Penneo rejects guarantees and applicable disclaimers in the documentation that connects the subscribers and relying third parties in certificates.

Penneo guarantees the subscriber, at least:

- Not factual errors in the information in the certificates, known or made by the Certification Authority.
- No factual errors in the information in the certificates, due to lack of due diligence of the certificate request or to its creation.
- The certificates comply with all the material requirements established in the Certification Practice Statement.

9.6.4 Relying party representations and warranties

The relying parties guarantees that all obligations of the relaying party existing prior to the use of the qualified certificate will be properly fulfilled. These obligations and responsibilities are specified in this certification policy, in particular in chapter 4.5.2.

9.6.5 Representations and warranties of other participants

The Cloud provider and data centre co-location are subjects directly involved in the operations of Penneo's PKI and The Platform services based on a contract concluded between providers and Penneo. They must fulfil conditions for continuous services of Penneo's Platform services.

Penneo uses Infrastructure as a service (IaaS) and Time synchronisation from Cloud provider. It provides access to networking features, computers, and data storage space. IaaS gives Penneo the highest level of flexibility and management control over your IT resources. Time synchronisation is described in particular CP for time-stamp. The relationship is managed through AWS Service terms.

The relationship between the co-location data centre and Penneo is managed through Service agreement containing SLA.

9.7 Disclaimers of warranties

Penneo provides guarantees in accordance with chapter 9.6.

9.8 Limitations of liability

Penneo uses qualified PKI services based on this CP and CPS. Penneo is not responsible for damages if subscribers and relying parties have not fulfilled the obligations required by the legal regulation.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Under contract with a customer, the Parties are liable for damages in accordance with the general rules of Danish Law with the limitations set out below, always provided that the limitations apply only if the loss is not attributable to gross negligence or willful intent on the part of the Party committing the tort.

Apart from product liability, the total amount of damages that the Customer can claim from Penneo in accordance with a customer agreement is limited to the smaller of the following:

- the total payment that Penneo has received from the Customer in accordance with their agreement at the time of the claim, or
- EUR 3,500 per claim per year.

9.9 Indemnities

Penneo only provides indemnity, in relation to possible data breaches. Herein either party is obligated to indemnify the other Party for expenses and use of resources in connection with the fulfilment of the obligations of a Party in relation to a supervisory authority or the data subject, as well as fines imposed by a supervisory authority or a court in so far as these are caused by a breach of the other Party.

9.10 Term and termination

The Agreement takes effect on the date on which the subscriber accepts this Agreement.

There is a period of commitment for access to the Platform for customers that have a subscription with Penneo is 12 months.

Either Party may terminate the Agreement at a written notice of 3 months to expire at the end of the subscription period. 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.

Penneo's Standard Terms are publicly available at https://penneo.com/terms/

9.10.1 Term

This CP is valid based on information of CP publication and approval by Penneo's manager. This document can be replaced by a new version of CP.

The Agreement between Penneo and subscribers takes effect on the date on which the subscriber accepts the Penneo Order Confirmation or otherwise accepts this Agreement ("Time of Commencement").

9.10.2 Termination

Termination of this document can be made by Penneo's manager decision in the case:

- of new version of trust services
- termination of PKI services

9.10.3 Effect of termination and survival

This document is valid to the end of validity of last issued certificates based on the CP.

9.11 Individual notices and communications with participants

The types of personal data and categories of data subjects that Penneo is to process for a subscriber as part of the service delivered is according to the Terms and the Data Processing Agreement.

It is only the subscriber who decides which personal data is to be processed by Penneo and for which purposes this personal data may be processed.

Penneo processes the personal data only in accordance with documented instruction from the subscriber and in accordance with the Legislation in force at any time.

9.12 Amendments

Penneo document key: D5ASZ-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

Each Party may at any time with a reasonable prior written and reasoned notice demand amendments to the Data processing agreement if the amendment is necessary to observe the Legislation in force at any time.

The Data processing agreement may furthermore at any time be adjusted in accordance to the terms applicable for the service.

9.12.1 Procedure for amendment

See chapter of 1.5 of this document.

9.12.2 Notification mechanism and period

New version of this document will be published on Penneo's web pages.

9.12.3 Circumstances under which OID must be changed

OID's are published in this CP. OID's are based on international standard and are assigned to Penneo.

All OID's are mentioned in the certification policy and CPS issued by Penneo. The OID is included in related the certificate.

Circumstances for changing are based on Penneo's business changes, new version of certification policy which have some influence on certificate guarantees.

9.13 Dispute resolution provisions

The Parties (Penneo and subscribers) agree that the Agreement has been concluded in accordance with Danish law and that any dispute between the Parties must be settled in accordance with Danish law.

The Parties shall endeavour to settle disputes amicably through negotiation. If a dispute cannot be settled amicably, both Parties are entitled to bring the matter before the Copenhagen City Court in the first instance.

9.14 Governing law

Processes and activities are governed by Danish law.

9.15 Compliance with applicable law

Processes of Penneo's PKI services are in line with valid Danish regulations. Relationship between Penneo and the subscribers are signed and based on the agreement.

If a provision in the Agreement is declared illegal, invalid or unenforceable, the provision must in spite of this be enforced to the greatest extent possible in accordance with current legislation so that the subscribers original intention reflected. Such a provision does not affect the lawfulness or validity of other provisions.

Any provision in the agreement which according to its nature extends beyond the time when the Agreement ends in full or in part shall continue to apply and be binding on the subscribers.

9.16 Miscellaneous provisions

If a provision in the Agreement is declared illegal, invalid or unenforceable, the provision must in spite of this be enforced to the greatest extent possible in accordance with current legislation so that the subscribers original intention reflected. Such a provision does not affect the lawfulness or validity of other provisions.

Any provision in the agreement which according to its nature extends beyond the time when the Agreement ends in full or in part shall continue to apply and be binding on the subscribers.

9.16.1 Entire agreement

This document applies the trust service provided by Penneo where CAs under this document are being used.

9.16.2 Assignment

Not supported.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

9.16.3 Severability

Not supported.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not supported.

9.16.5 Force Majeure

If Penneo cannot provide its services in accordance with the Agreement as a result of force majeure, Penneo cannot be held liable for losses on account of that and the Customer cannot terminate the Agreement with immediate effect. If the accessibility to the Service is essentially impossible due to force majeure and this lasts for more than 30 days, either Party may terminate the Agreement in writing with immediate effect but cannot in that connection advance any claims against the other Party.

Penneo must inform the Subscriber without undue delay if a force majeure situation arises. Force majeure is a matter on which Penneo has no influence and which Penneo cannot bypass with reasonable financial and practical measures. Force majeure is for example war, mobilisation, terrorist attack, failure/breakdown of public electricity supply, strike, fire, flood etc.

9.17 Other provisions

Chapter is not relevant for this document.

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

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

Penneo document key: D5AS7-PU89J-2QTNJ-QJOHM-56PGT-N8LBX

This document is digitally signed using **Penneo.com**. The signed data are validated by the computed hash value of the original document. All cryptographic evidence is embedded within this PDF for future validation.

The document is sealed with a Qualified Electronic Seal. For more information about Penneo's Qualified Trust Services, visit **https://eutl.penneo.com**.

How to verify the integrity of this document
When you open the document in Adobe Reader, you should see that the document is certified by **Penneo A/S**. This proves that the contents of the document have not been modified since the time of signing. Evidence of the individual signers' digital signatures is attached to the document.

You can verify the cryptographic evidence using the Penneo validator, **https://penneo.com/validator**, or other signature validation tools.