CPS and CP for Root and Intermediate CA

Version history

Version	Date of release	Approved by (Title and name)	Comments
1.7	26th November 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	17th October 2025	COO / Christel Victoria Høst	Updated RSA key size for subordinate certificates under 6.1.5
1.5	26th May 2025	COO / Christel Victoria Høst	Updated company address under 2.2.1
1.4	30th December 2024	Information Security Manager / Fredrik Lernevall	Grammatical improvements and clarification of descriptions for increased readability. Contact persons under 1.5.2 and 1.5.3. Updated Certificate application processing 4.2 and subsections. Retention period under 5.5.2 and 6.3.1.
1.3	7th March 2024	Information Security Manager / Fredrik Lernevall	Intermediate CA added to name. Section 1.2 updated to include intermediate CA. Intermediate CA Certificate Profile transferred from internal repository to chapter 7.1. Validity of RootCA corrected in Chapter 7.
1.2	23rd January 2023	Information Security Manager / Fredrik Lernevall	Updated URL for Penneo's Trust Center under section 2.2.1
1.1	21st November 2022	Information Security Manager / Fredrik Lernevall	Administrative changes
1.0	23rd June 2022	Information Security Manager / Fredrik Lernevall	First release

OID of Root CA Certification Policy and Certificate Practise Statement:

1.3.6.1.4.1.57006.1.1.1.1.1

Version: 1.7

1. Introduction

The document describes and specifies the procedures, activities and rules that apply to Penneo's Certification Policy (hereinafter CP) for Root Certification Authority (hereinafter Root CA).

Penneo as a qualified provider implements the CPS and CP for Root CA in the trust building services of Public Key Infrastructure (hereinafter PKI) and in issuing self-signed qualified Root CA certificate.

Penneo's trust services shall be compliant with eIDAS and EU regulations.

Penneo implements its PKI infrastructure in Penneo's application (the Platform), which is partly hosted in a co-location data center and partly built in a public cloud environment for higher availability. 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.

The CPS and CP for Root CA issuing qualified self-signed certificate for describes the facts related to the life cycle processes of the issued Root CA certificate and follows the structure, the model of the valid standard RFC 3647, taking into account the valid technical standards and principles. Technical requests and detailed information about this problematic are described in internal documentation.

1.1. Overview

The document is divided into nine chapters:

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, and 3) description of the implementation of Penneo's services.

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 of 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 completeness of certificate life cycle: the application for issuance, the processes of issuing certificates, confirmation and approval of certificates, including notification of certificate issuance. Chapter solves the process of usage of electronic seals etc.

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 explains the issue of computer and network security, their principles and required control mechanisms.

Chapter 7 - describes certificate profiles of electronic seals.

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 Practice Statement and Certification Policy of Root and Intermediate CA issuing qualified certificates for Penneo's CAs.

OID of Root CA Certification Policy and Certificate Practise Statement:

1.3.6.1.4.1.57006.1.1.1.1.1

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.

1.3.1.1 Root Certification Authority

The Root Certification Authority (Root CA) is offline, meaning it is neither connected to an internal nor external network. The Root CA is physically formed by a dedicated computer and a secure cryptographic module containing a private key.

The root CA does not provide any services to internal or external subscribers.

The Root CA is physically formed by a dedicated computer and a secure cryptographic module containing a private key. The all process of key generation and implementation to the Penneo’s hardware and software architecture is managed during the initialization process.

Penneo’s PKI servicers remove or disable all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

The PKI infrastructure is used for all qualified services provided through Penneo’s qualified trust service.

1.3.1.2. Certification Authorities issuing certificates

Root CA issues certificates for subordinates CA for electronic signature and seal and Time stamp CA only. The Subordinate CAs provide Services to Subscribers - certificates for remote electronic signing and certificates for remote electronic sealing. Time-stamp authority issues time-stamps for confirmation of date and time validity.

1.3.2. Registration Authority

As a registration authority serves internal processes performed by Penneo's responsible employees.

1.3.3. Subscribers

The certificate is issued by Penneo company for the qualified Root CA exclusively. Penneo is the holder of the private key and the certificate and issues this certificate for required trust services.

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 electronic Penneo's PKI Services according to this document.

1.3.5. Other participants

Other participating entities may be supervisory authorities or law enforcement authorities.

Based on requirements for continuous operations and ensuring the provision of qualified and remote services, Penneo uses an external data centre and the Platform is implemented to a cloud solution. These services are governed by a contract between Penneo and the parties.

1.4. Certificate usage

1.4.1. Appropriate certificates uses

Root CA certificates may be used to verify Certificates issued by that root CA only and:

- verify the lists of revoked certificates (CRL) issued by this root CA;
- to verify certificates of electronic seals, signature, time-stamps and certificate revocation lists (CRLs) issued by subordinate certification authorities.

The application of the certificate is included in the certificate.

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 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 approved 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.

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.
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
SmartCard-HSM	The SmartCard-HSM is a lightweight hardware security module in a smart card and form factor. It provides a remote-manageable secure key store for RSA and ECC keys.The SmartCard-HSM is USB Token, which is effectively a chip card interface device (CCID) compliant card reader combined with the smart card chip in a single device.

Acronyms

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

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;
- 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: http://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 every 6 months, with a validity time of one year. 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

The naming scheme of Penneo’s trust services is approved and implemented by responsible Penneo employees or Penneo’s managers.

3.1.1. Types of names

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

3.1.2. Need for names to be meaningful

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

3.1.3. Anonymity or pseudonymity of subscribers

No anonymity or pseudonymity is supported.

3.1.4. Rules for interpreting various name forms

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

3.1.5. Uniqueness of names

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

3.1.6. Recognition, authentication, and role of trademarks

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

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

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

Methods of private key ownership is realized through a complex internal process:

- unambiguous identification of Penneo's specialists (administrators and operators) before initialization process;
- verification of the cryptographic module, its delivery and transportation and its initialization;
- fulfilling of described internal processes for cryptographic module’s initialization (rooms, participants, roles);
- participation of an auditor and his/her verification of processes;
- participation minimally of two responsible and determined employees for manipulation with generated keys.

One employee has no possibility to generate new keys for the Root CA.

3.2.2. Authentication of organizational identity

Penneo company performs all activities for root keys generation and uses its own trademarks and names described in internal document for initialization process.

3.2.3. Authentication of individual identity

Authentication of the identity verification is performed through defined rules and procedures of the Penneo's internal registration and initialization process.

Employees responsible for root key pair generation are defined and approved by Penneo's manager.

The process is described in internal documentation under Key Management documentation.

3.2.4. Non-verified subscriber information

There exists verified information only.

3.2.5. Validation of authority

No relevant for this document.

3.2.6. Criteria for interoperation

Penneo's CAs (including TSA) and PKI structure is created for the needs of subscribers implementing a remote qualified electronic time stamp, signature and sealing. It does not implement connections with other CA or other ways of interoperability.

3.3. Identification and authentication for re-key request

Penneo's Root CA issues self-signed certificate for Root CA and certificates for subordinates CAs - CA for qualified electronic signature and seals and Time stamp CA. Penneo's CA services do not support the act of re-key.

A new root certificate is always issued and the steps are the same as during initialization process.

3.3.1. Identification and authentication for routine re-key

The identification and authentication requirements are the same as during initialization process.

3.3.2. Identification and authentication for re-key after revocation

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

3.4. Identification and authentication for revocation request

The requests for revocation is implemented through a request from Penneo's authorized and responsible employee based on specified internal conditions. See chapter 4.9.2. and 4.9.3.

4. Certificate life-cycle operational requirements

4.1. Certificate application

4.1.1. Who can submit a certificate application

The request for the issuance of the Root CA certificate may be submitted by Penneo's manager or responsible employees approved by Penneo's manager. The initialization processes are managed by Penneo's security manager and supported during keys generation by relevant Penneo employees as well as at least an internal and external witness.

4.1.2. Enrollment process and responsibilities

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

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

Penneo's responsible employees check and verify mentioned data according to written request and initiate the key generation process.

Penneo's responsible employees have to perform activities to publish the certificate and implement the certificate in Penneo's PKI services for use in the Platform's automated processes.

The process complies with legal standards and Penneo implements the process according to internal procedures.

4.2. Certificate application processing

4.2.1. Performing identification and authentication

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

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

4.2.2. Approval or rejection of certificate application

The process of certificate rejection or approval is based on the appropriate identification of the subscriber facilitated by the RA. Penneo's Platform checks the subscriber ID and identity data provided by the RA in an e_token. The Platform verifies that the e_token is valid, signed by the RA's private key, and whether the identification data is compliant with the requirements for the qualified certificate profile.

If the e_token does not contain the necessary data or cannot be validated, the request is rejected. If identification data is not provided by the RA within the subscriber's session, the request is also rejected. In both cases, an error is shown to the subscriber on the platform.

In terms of issuing root CA or subordinate CAs certificates, the complete process is based on Penneo's internal security procedures and all such activities are documented.

4.2.3. Time to process certificate applications

Penneo's security manager will review applications in a timely manner and ensure applications are appropriately processed.

4.3 Certificate issuance

4.3.1. CA actions during certificate issuance

During the process of certificate issuance, the written request is verified and checked by Penneo's responsible employees. If all controls are met, the keys are generated in a secure way. A written protocol is signed by all participants.

The process of key pair generation and certificate issuance is managed and fully automated and performed in a secure hardware cryptographic module.

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

The Penneo's manager or responsible employee ensures the certificate publication on Penneo's web pages and its implementation to Penneo's PKI services.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

Penneo manager or responsible employee confirms the information on the issuance and acceptance of the certificate and approves the certificate usage in remote automated process created for electronic signature, time stamp and sealing.

Root CA is switched off after:

- issuing and implementation of Subordinate CAs certificates keys and certificates acceptance,
- issuing of CRL,
- implementation of Root and Subordinate CAs to PKI services and Penneo's applications (the Platform),

- backup is performed.

Root CA is disconnected from network and the cryptographic module situated on secure place under Penneo's controls.

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 document(s) that the subscriber signed through Penneo's Platform.

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

Subscriber (Penneo's determined and responsible employees) uses private key and certificate corresponding to:

- processes mentioned in the CP/CPS;
- relating legal purposes, internal documentation and EU legislation;
- conditions mentioned within this CP/CPS in such a way that it cannot be misuse;
- compliance with the provisions on the usage of the private key and certificate under the Penneo's the Platform services and agreements;
- backup of the private key, escrow and setup storage and protection of the hardware cryptographic module;
- verification if Root CA is disconnect from network, used cryptographic module is securely stored and is not possible to misuse them.
- written protocols is written and signed in case of unexpected events and every manipulation with the private key.

Penneo performs immediately actions, if:

- some suspicion exists about misuse of private key;
- if exists some irregularities that the data in the certificate is not complete or accurate.

In those cases - Penneo's responsible employees have to interrupt the processes of the Penneo Platform services and stop usage of the private key. After analysis of the event to perform correction steps.

4.5.2. Relying party public key and certificate usage

Before usage of the Root CA certificate relying parties have to download relating certificates of Penneo CA's web pages and verify content of certificates, name, fingerprint and validity. Relying parties have to verify if the root certificate is still valid and qualified for providing trust services.

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 with a new name.

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

4.9.1. Circumstances for revocation

Responsible Penneo's employees immediately perform revocation, if:

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

4.9.2. Who can request revocation

Penneo’s responsible employees or Penneo’s manager can request revocation and start revocation process.

4.9.3. Procedure for revocation request

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

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

Penneo's manager approves issuing of the new certificate.

After issuing of the certificate:

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

4.9.4. Revocation request grace period

Revocation request must be solved for Penneo Platform services immediately.

4.9.5. Time within which CA must process the revocation request

Time within which CA must process the revocation request of the certificate is immediately and and new CRL has to be issued.

4.9.6. Revocation checking requirement for relying parties

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

4.9.7. CRL issuance frequency

The Root CA issues CRL twice a year, with validity time one year.

4.9.8. Maximum latency for CRLs

The CRL of root CA is always issued no more than half a year after the issuance of the previous CRL.

4.9.9. On-line revocation/status checking availability

For Root CA is not present on-line certificate status - root CA is offline.

4.9.10. On-line revocation checking requirements

All requirements are based on verification of the information placed on Penneo’s web pages. Root CA is offline.

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

Certificates issued by the Root CA are in the certificate repository, inside certificates are Penneo attributes and identifications.

The all processes of a certificate status verification is performed by the Platform cooperating with PKI services and is fully automatic and complex without interruption.

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

4.10.2. Service availability

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

4.10.3. Optional features

Optional features are not provided.

4.11. End of subscription

The Root CA issuing certificates for subordinate CAs, performs services and is responsible to perform the all promised activities mentioned inside this CP/CPS for the all time period of certificates are valid (for the period of validity of the last issued Certificate).

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 secure cryptographic modules and defined suppliers procedures for completion of the CAs keys during recovery. Parts of keys are encrypted and is not possible to transfer them in readable forms. The private key after activation never leaves the 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 Computer 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);
- 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 Officers
- System Administrators
- System Operators
- 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. Personal 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 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.

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 Qualified 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.

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 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 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.

5.7.5 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.

5.8 CA or RA termination

5.8.1. CA termination

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:

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.

5.8.2. RA termination

Registration authority is not used.

6. Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Prior to generating key pair using Penneo’s devices, Penneo ensures that hardware can be trusted by verifying no evidence of tampering has occurred as specified by the hardware provider.

The process of generating CA key pair involves writing a key ceremony script that must be followed during the key ceremony.

For the generation of Root CA key pair an external Qualified Auditor must be present in order to verify the correct completion of the defined script.

Information that will be recorded in the script will include:

- key ceremony participants;
- locations;
- access rights of participating persons and Penneo's responsible employees;
- how the cryptographic modules are prepared - verification of the integrity of the packaging and equipment;
- description of cryptographic module;
- initialisation process of the generation of keys is verified step by step;
- time of each performed step;
- signature of key ceremony participants.

6.1.2 Private key delivery to subscriber

For private key of Root CA is not relevant.

Private keys are saved in the hardware cryptographic module and root CA is offline.

6.1.3 Public key delivery to certificate issuer

Is not relevant. Root CA key pair is generated in cryptographic module automatically and the root CA certificate is immediately implemented to a tree of Penneo's PKI services as a part of Penneo’s application (the Platform) for qualified remote electronic signature, time-stamp and sealing.

The certificate is published on Penneo's web pages.

6.1.4 CA public key delivery to relying parties

CA public keys are part of CA certificates. CA certificates are published on Penneo's web pages.

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. Keys pair 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 cryptographic 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

Private keys are saved to secure cryptographic modules under Penneo's controls.

Subscribers use secure cryptographic modules that are implemented to infrastructure for automated Penneo’s Platform services.

6.2.1 Cryptographic module standards and controls

Standard for root CA cryptographic 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 secure cryptographic modules which are certified by Common Criteria as well (Common criteria level 4+).

Before initialisation procedure Penneo verifies if all secure cryptographic 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 primary purpose of the key management is to maintain the assurance of confidentiality and integrity for any cryptographic key. It requires an efficient and secure key management process (key distribution, key exchange, key storage, key archive), which must be documented including its adhering roles and responsibilities. The secure and proper management of cryptographic keys is critical to the effective and proper use of encryption techniques.

The control over the private key is split using a n-of-m scheme for the private credentials. In such a scheme m defined and responsible employee are given a private credentials and n defined and responsible employee must come together to activate the private key.

Responsible employees do not perform a key life cycle operations without cooperation with other defined employee.

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

6.2.3 Private key escrow

Not applicable

6.2.4 Private key backup

The secure cryptographic environment supports encrypted key backup and restore using mechanisms that can be set during cryptographic modules initialisation.

The mechanisms ensure that cryptographic material is never exposed in plain. Any media containing private key components used for loading cryptographic keys must be maintained in a secure location and accessible only to authorized employees. When removed from the secure storage location devices containing key components are for the minimum practical time necessary to complete the key-loading process.

The media upon which a component resides must be physically safeguarded at all times when removed from secure storage.

6.2.5 Private key archival

After the expiration of the private keys of the root certification authority or after Penneo’s PKI termination keys are destroyed, including the backups and the cryptographic module is initialised.

6.2.6 Private key transfer into or from a cryptographic module

Transferring of the keys should be minimised.

Transfer of the private key from back-up into cryptographic module is possible during recovery process. The private key leaves the cryptographic module in encrypted form based on backup and recovery processes specified in internal documentation only.

Authentication minimally two responsible Penneo's employees is necessary for recovery purposes based on internal processes. Written protocol is created and approved by Penneo's manager.

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 cryptographic modules that meet the requirements of the legislation for trust-building services.

For cryptographic module activation and initialization minimally two Penneo’s responsible employees have to cooperate.

Subscribers private key is stored in the secure cryptographic module and after signature is the private key deleted.

6.2.8 Method of activating private key

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

Activation of private keys of the CAs certificates which are stored in secure cryptographic modules is performed with the direct personal participation of at least two Penneo’s responsible persons authorized by Penneo’s management. 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 the root CA private key is performed with the direct personal participation of at least two Penneo’s responsible employees authorized by Penneo’s management.

Written protocols are made for the deactivation.

First step before deactivation is to stop the Platform usage and realise steps for the new keys generation.

6.2.10 Method of destroying private key

Destroying of private keys is done if:

- the secure cryptographic module has to be used for other purposes;
- the validity of secure cryptographic module ends;
- the Penneo terminates trusted services;
- new subsequent certificate is issued;
- revocation or expiration of certificates.

Destroying is performed by means and tools of the hardware secure cryptographic modules managed by Penneo.

External media on which backups of the private keys are stored are also destroyed. The destroying, consisting in the physical destroying of these carriers, takes place with the direct personal participation of at least two Penneo's responsible employees approved by Penneo's manager.

6.2.11 Cryptographic Module Rating

Penneo uses cryptographic modules for key pairs generation and storage of CAs private keys cryptograhic modules that meet the requirements of the legislation for trust-building services (The Common Criteria EAL 5 and 4+).

The cryptographic modules are implemented to Penneo’s application 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

Operational period of root certificates is defined in the Root CA certificate. There is no difference between operational and key pair usage period.

The last subscriber certificate will be issued in date prior to expiration of the Root CA certificate. A new Root CA certificate replacing the old one will be issued in time to support Penneo's trust services.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data is generated during initialisations processes of a particular secure cryptographic module and key pairs generation of the particular CA.

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

6.4.2 Activation data protection

Activation data is distributed among responsible Penneo's employees in specified form only and are saved in secure places. Protection of activation data 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.

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 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

Root CA

The root Certificate is issued according to this CP/CPS and is 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. It is the self-signed certificate.

Penneo uses certificate profiles described in internal documentation - Certificate profiles. Commonly is used table:

Basic certificate fields:

#	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	version		Version of the certificate that complies with with X.509 standard, version 3.	v3 (0x2)	Mandatory
2	serialNumber		Unique serial number of the certificate assigned by the CA.	Positive integer explicitly assigned by the CA	Mandatory
3	signatureAlgorithm		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	minimum SHA256WithRSAEncryption (1.2.840.113549.1.1.11)	Mandatory
4	issuer		Distinguished Name of the Issuer's certificate.	X.501 type Name	Mandatory
5	validity			ASN.1 SEQUENCE	
6		notBefore	The date on which the certificate validity period begins	UTCTime	Mandatory
7		notAfter	The date on which the certificate validity period ends.	notBefore + 25 years	Mandatory
8	subject		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See Subject Field below for details.	X.501 type Name	Mandatory
9	subjectPublicKeyInfo			ASN.1 SEQUENCE	
10		algorithm	Identifies the algorithm with which the key is used.	minimum SHA256WithRSAEncryption (1.2.840.113549.1.1.11)	Mandatory
11		subjectPublicKey	Public key of the associated entity.	minimum 3072 bits for RSA keys	Mandatory
12	extensions		Sequence of one or more certificate extensions. See Certificate Extenstions below for details.	ASN.1 SEQUENCE	Mandatory
13	signatureValue		Qualified electronic seal of the trust service provider Intermediate CA.	Signature represented as BIT STRING	Mandatory

Issuer Field:

#	Item	Description	Value	Mandatory / Optional / Critical	Note
1	commonName	Identification of the subscriber within the CA.	Penneo Qualified Root CA **MM/YY/ALG**	Mandatory	• MM is the number of month in which the CA certificate was issued • YY is the last two digits

#	Item	Description	Value	Mandatory / Optional / Critical	Note
					from year number in which the CA certificate was issued • ALG identified public key algorithm used for CA certificate (e.g. RSA)
2	organisationName	Organisation name where the subscriber is employed or which is represented by the subscriber.	Penneo A/S	Mandatory	
3	organisationIdentifier	Identification number of the organisation.	NTRDK-35633766	Mandatory	id-etsi-qcs-SemanticsId-Legal as defined in ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
4	countryName	Country code.	DK	Mandatory	Two characters based on ISO 3166

Subject Field (the same as Issuer Field)

#	Item	Description	Value	Mandatory / Optional / Critical	Note
1	commonName	Identification of the subscriber within the CA.	Penneo Qualified Root CA **MM/YY/ALG**	Mandatory	• MM is the number of month in which the CA certificate was issued • YY is the last two digits from year number in which the CA certificate was issued • ALG identified public key algorithm used for CA certificate (e.g. RSA)
2	organisationName	Organisation name where the subscriber is employed or which is represented by the subscriber.	Penneo A/S	Mandatory	
3	organisationIdentifier	Identification number of the organisation.	NTRDK-35633766	Mandatory	id-etsi-qcs-SemanticsId-Legal as defined in ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
4	countryName	Country code.	DK	Mandatory	Two characters based on ISO 3166

Intermediate CA

Basic Certificate Fields

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with with X.509 standard, version 3.	v3 (0x2)	Mandatory
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer explicitly assigned by the CA	Mandatory
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**sha512withRSAandMGF1**(inherited from the issuing CA)	Mandatory
4	**issuer**		Distinguished Name of the Issuer's certificate.See **Issuer Field** below for details.	X.501 type Name	Mandatory
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	Mandatory
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **10 years**	Mandatory
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field.See **Subject Field** below for details.	X.501 type Name	Mandatory
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	**sha512withRSAandMGF1**	Mandatory
11		**subjectPublicKey**	Public key of the associated entity.	RSA 4096 bits	Mandatory
12	**extensions**		Sequence of one or more certificate extensions.See **Certificate Extenstions** below for details.	ASN.1 SEQUENCE	Mandatory
13	**signatureValue**		Qualified electronic seal of the trust service provider Root CA. (Self-signed)	Signature represented as BIT STRING	Mandatory

Issuer Field (issued from Root CA)

	Item	Description	Value	Mandatory / Optional / Critical	Note
1	**commonName**	Identification of the subscriber within the CA.	Penneo Qualified Root CA **MM/YY/ALG**	Mandatory	• **MM** is the number of month in which the CA certificate was issued• **YY** is the last two digits from year number in which the CA certificate was issued• **ALG** identified public key algorithm used for CA certificate (e.g. RSA)
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Penneo A/S	Mandatory	
3	**organisationIdentifier**	Identification number of the organisation.	NTRDK-35633766	Mandatory	id-etsi-qcs-SemanticsId-Legal as defined in ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
4	**countryName**	Country code.	DK	Mandatory	Two characters based on ISO 3166

Subject Field

	Item	Description	Value	Mandatory / Optional / Critical	Note
1	**commonName**	Identification of the subscriber within the CA.	Penneo Qualified Intermediate **SUB** CA **MM/YY/ALG**2 intermediate CAs:• Penneo Intermediate **Qualified TSA** CA MM/YY/ALG• Penneo Intermediate **Qualified** CA MM/YY/ALG	Mandatory	• **SUB** is the name of the intermediate CA• **MM** is the number of month in which the CA certificate was issued• **YY** is the last two digits from year number in which the CA certificate was issued• **ALG** identified public key algorithm used for CA certificate (e.g. RSA)
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Penneo A/S	Mandatory	
3	**organisationIdentifier**	Identification number of the organisation.	NTRDK-35633766	Mandatory	id-etsi-qcs-SemanticsId-Legal as defined in ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
4	**countryName**	Country code.	DK	Mandatory	Two characters based on ISO 3166

7.1.1 Version number(s)

see Chapter 7

7.1.2 Certificate extensions

RootCA

#	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	AuthorityKeyIdentifier				Not critical Mandatory
2		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	
3	SubjectKeyIdentifier		Identification of certificates that contain a the subject public key.	160 bit SHA-1/SHA-512 hash function on the value of the public key of the subscriber's certificate	Not critical Mandatory
4	KeyUsage		Defines the purpose of the key contained in the certificate.	keyCertSign cRLSign	Critical Mandatory
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.	2.5.29.32.0 (anyPolicy)	
7	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
8		CA	Identifies whether the subject of the certificate is a CA.	True	

Intermediate CA

	Extension	**Sub-fields in SEQUENCE**	**Description**	**Content**	**Mandatory / Optional / Critical**	**Note**
1	**AuthorityKeyIdentifier**				Not critical Mandatory	
2		**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		
3	**SubjectKeyIdentifier**		Identification of certificates that contain a the subject public key.	160 bit SHA-1/SHA-512 hash function on the value of the public key of the	Not critical Mandatory	

				subscriber's certificate		
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	`keyCertSign` `cRLSign`	Critical Mandatory	RFC 5280
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.	2.5.29.32.0 (anyPolicy)		
7		**policyQualifiers**	Pointer to a Certification Practice Statement (CPS) published by the CA.	**userNotice**: This is a qualified certificate for electronic seal according to Regulation (EU) No 910/2014.		
8	**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	
9		**cA**	Identifies whether the subject of the certificate is a CA.	True		
10		**pathLenConstraint**	Maximum number of non-self-issued intermediate certificates that may follow this certificate in a valid certification path.	0		Only end e certificate be issued the Intermedia CA.
11	**CRLDistributionPoints**		Identifies how CRL information is obtained.	URI	Not critical Mandatory	
12	**AuthorityInformationAccess**		Indicates how to access information and		Not critical Mandatory	

			services for the issuer of the certificate.			
13		**id-ad-calssuers**	Access CA certificate.	URI		

7.1.3 Algorithm object identifiers

Algorithm is defined in related technical standards.

7.1.4 Name forms

Name forms correspond to Penneo identification. See chapters from 3.1.1. to 3.1.4.

7.1.5 Name constraints

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

7.1.6 Certificate policy object identifier

OID of this CP/CPS is defined based on related technical standards and used in the 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 an alternative to CRL in LDAP Penneo can use WEB services or other services passing for certificate 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	Mandatory / Optional / Critical	Note
1	version		Version of the certificate that complies with with X.509 standard, version 3.	v2 (0x1)	Mandatory	
2	signatureAlgorithm		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	sha512withRSAandMGF1	Mandatory	Compliant with ETSI TS 119 312 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
3	issuer		Distinguished Name of the	X.501 type Name	Mandatory	Refer to the Issuer field of

#	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical	Note
			Issuer's certificate.			the CA certificate.
4	thisUpdate		Issue date of the CRL	UTCTime	Mandatory	
5	nextUpdate		The date by which the next CRL will be issued.	UTCTime	Mandatory	
6	revokedCertificates		List of revoked certificates.		Mandatory if there is at least one certificate revoked. Not present if the list of certificates is empty.	
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	Mandatory	

CRL Extensions

#	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	crlReason		Reason of the revocation.	unspecified (0) keyCompromise (1)	Not critical Optional

#	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
				cACompromise (2) affiliationChanged (3) superseded (4) cessationOfOperation (5) certificateHold (6) removeFromCRL (8) privilegeWithdrawn (9) aACompromise (10)	Mandatory for certificates in the list of revoked Certificates
2	AuthorityKeyIdentifier				Not critical Mandatory
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	Not critical Mandatory

7.2.1 Version number(s)

see Chapter 7.2

7.2.2 CRL and CRL entry extensions

see Chapter 7.2

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 a Qualified 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.

8.1 Frequency or circumstances of assessment

Compliance to eIDAS requirements is audited every two years by a Qualified Auditor.

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

The Penneo is obliged to allow authorities who in accordance with the legislation in force at any time have access to the facilities of the subscribers and the Penneo or representatives who act on behalf of the authority access to the physical facilities of the Penneo against due identification and the prior signing of a non-disclosure declaration.

Penneo also performs internal audits.

8.2 Identity/qualifications of assessor

Penneo’s Trust Service must be audited by a Qualified Auditor. The Qualified Auditor must be trained for auditing such services and be independent of the audit subject. The Qualified 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.

Applicable fees will be stated in the Terms of the contract between Penneo and Subscriber.

9.1.2 Certificate access fees

Certificates access is provided by Penneo free of charge.

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 subscriber's 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 in order to secure sufficient resources to keep operations running, as well as further develop the trust service. As a listed company, Penneo releases quarterly financial reports in addition to the annual report. Released financial reports are found on Penneo's homepage.

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
- 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

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.

9.6.2 RA representations and warranties

Not applicable.

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

Relying parties follow the CP according to which the Certificate was issued.

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.

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.

Penneo disclaims liability for any indirect loss or consequential loss including, but not limited to, business interruption, loss of profits, loss of the Customer’s Data and goodwill with the Customer.

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
- DKK 25,000 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

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.

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.