Disclosure Statement for PKI

Version history

Version	Date of release	Approved by (Title and name)	Comments
1.2	30.12.2024	Information Security Manager / Fredrik Lernevall	Improved readability. Updated reference to amended eIDAS.
1.1	25.01.2023	Information Security Manager / Fredrik Lernevall	Updated the URL for Penneo's Trust Center in section 6.1
1.0	22.11.2022	Information Security Manager / Fredrik Lernevall	First release

Disclosure Statement for PKI is the document required by European standard ETSI EN 319 411-1, related to the certification services offered by the Penneo as the Trust service provider (TSP).

In the following, the certification services is also referred to as "CA services" (Certification Authority services).

The Regulation (EU) No 910/2014 amended by Regulation (EU) 2024/1183 (hereafter referred to as "eIDAS").

The purpose of this document is to summarise the main processes and steps performing Penneo's CA services for subscribers and Relying Parties. This document does not substitute the Certification Practice Statement (CPS) or particular Certification Policies and Practice Statements.

1. TSA Contact Information

The CAs are operated by Penneo A/S. Penneo's address is the following:

Penneo A/S

Enghavevej 40

1674 Copenhagen V

Denmark

Penneo can also be contacted on the following email address:

trustservice@penneo.com

2. Certificate type, validation procedures and usage

Penneo’s PKI services issues qualified certificates according to European standards:

- ETSI EN 319 411-1
- ETSI EN 319 411-2
- ETSI TS 119 495
- ETSI 119 431 - 1 and 2
- and other related standards.

Certificates are offered to the private/natural persons and legal organizations/companies.

Certification Policies and Certification Practice Statement for certificates are published on Penneo’s web pages and publicly available.

2.1. Certificates type

- Penneo's Root certification authority (RSA key 4096 bits, signature algorithm sha512withRSAandMGF1) issues, in accordance with the requirements of technical standards and current legislation, certificates solely to the subordinates CAs - for remote electronic signature and seal (RSA key 4096 bits, signature algorithm sha512withRSAandMGF1**)** and for Time Stamp (RSA key at least 2048 bits, signature algorithm sha512withRSAandMGF1).
- Penneo's certification authority for remote electronic signature and seal (RSA key 4096 bits, signature algorithm sha512withRSAandMGF1) is intended for issuing certificates for qualified certificates for remote electronic signature

and electronic seal to subscribers (with RSA key at least 2048 bits, signature algorithm at least sha256WithRSAEncryption).

2.2. Certificate usage

Penneo issues certificates to subscribers, who use the Penneo Platform for remote electronic signature, sealing and time stamps. Subscribers access the platform via internet connection.

Penneo uses services of external companies in the role of Registration Authorities (RA).

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

Qualified certificates are used solely for remote electronic signatures, seals and time stamps.

Penneo's PKI services and the Platform are in compliance with Regulation (EU) No 910/2014 amended by Regulation (EU) 2024/1183 (hereafter referred to as "eIDAS"), including associated implementing regulations and technical standards.

2.3. Verification/validation procedures

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

3. Obligations of Subscribers

A certificate application can be submitted by a subscriber. There are two types of subscribers for the remote electronic signature service:

1. Customers - means a company, organisation or other legal entity, on behalf of which an employee of the company, organisation or other legal entity has accepted Agreement between Penneo and Customers either directly or by accepting the Penneo Order Confirmation.

   A customer authenticates on the Platform, then uploads documents for electronic signature and specifies names and emails of signers. Signers receive a request for signature via email, containing a unique link to the Platform.

2. Signers (could be employees working on behalf of the Customer’s company, organization or other legal entity, employees of other Customers or other natural persons) receive a request for signature via email, containing a unique link to the Platform. Signers are not necessarily Penneo's customers but Penneo has an agreement with them, since they accept the terms before they sign. Signers are informed about Penneo’s qualified trust services in the Platform for remote electronic signatures during the signing process.

The subscriber basic obligations for the certificate include:

- To provide truthful and complete information when registering with a particular RA/IP;
- To immediately inform the RA/IP of personal data changes in the agreement;
- To fulfil the agreement between Penneo and the subscriber;
- To become acquainted with particular CP, CPS and legal procedures before electronic signature is used;
- To check/verify whether the displayed information are correct and confirm information in the Penneo Platform;
- To immediately stop the process of electronic signature and terminate the use of the relevant private key, especially in the case of private key compromise or suspicion that the private key has been abused during creation of electronic signature.

4. Obligations of Relying parties

Relying parties may only use the public key of the certificate for the purposes described in the relying party agreements with Penneo and as described in the CPS and, Terms and Conditions including necessary conditions for the Platform usage.

5. Limited warranty and disclaimer

Penneo rejects any other guarantee that is not enforceable under the laws, except the ones covered in applicable CP for remote electronic signature and seal.

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

Penneo guarantees the subscriber, at least:

- Not factual errors in the information (subscriber's data) in the certificates, known or made by the Certification Authority.
- No factual errors in the information (subscriber's data) 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.

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

Penneo ensures accessibility to the Platform during the term of the Agreement as stated - uptime of 99.9%

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

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

5.1. Limitations of liability

Penneo uses qualified PKI services based applicable CPS and related CPs for remote electronic signature and seal. 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 subscriber, 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 wilful 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 subscriber's Data and goodwill with the subscriber.

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

- the total payment that Penneo has received from the subscriber in accordance with their agreement at the time of the claim, or
  - DKK 25,000 per claim per year.

6. Applicable agreements and policies

Penneo is responsible for all processes performed in the Platform including Penneo's PKI Services.

Activities of Penneo and the Platform are based on a contract between registration authorities (RA) in the role of Identity Providers (IP). Penneo has to manage the collaboration with RA/IP companies and relies on RA/IP issue subscriber identifiers.

The relationship between the subscriber and Penneo including Penneo's PKI services is governed by the relevant agreements:

- Standard terms and data processing agreement
- provisions of applicable certification policies and Practice Statements.

6.1. CPS and CP (Certificate Practice Statement and Certification Policies)

Penneo PKI service is based on the following CPS, and related CP:

- Practice statements:
  - Certificate Practice Statement and Certificate Policy for Root CA;
  - Certificate Practice Statement for Subordinates CAs;
  - Trust Service Practice Statement, with attachments for electronic signature, seal and timestamp;
- Certification Policies for:
  - remote and qualified electronic signature;
  - remote and qualified electronic seal;
  - remote and qualified electronic time stamp;
  - Certificate Practice Statement and Certificate Policy for Root Certification authority.
- Disclosure Agreements:
  - Disclosure agreement for PKI;
  - Disclosure agreement for Time-stamp.

The documents can be found on the Penneo Web page https://eutl.penneo.com/

7. Privacy Policy

Penneo addresses personal data protection in a consistent manner and compliance with the regulation, EU Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Penneo must implement the necessary technical and organizational security measures to prevent personal data from 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 valid Legislation.

8. Refund policy and claims

The applicable refund policy is stated governed by the terms of the agreement entered by the subscriber and Penneo.

9. Applicable law, complaints and dispute resolution

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 District Court of Copenhagen in the first instance.

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

Penneo issues qualified certificates in accordance with eIDAS.

To ensure compliance to eIDAS, Penneo issues certificates based on a certificate profile related to standard X.509 version 3 in compliance with norms and standards:

- 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;
- and other ETSI standard relevant for remote and qualified electronic signature and seal.

Any complaint shall be sent to trustservice@penneo.com

10. Trust marks, audit, repository licenses

Penneo has been audited by a Qualified Auditor against applicable requirements based eIDAS and subsequently accepted as a Qualified Trust Service Provider (QTSP). An audit will be performed by a Qualified Auditor every two years to ensure continued compliance to applicable standards as dictated by eIDAS.

Penneo's policy ensures that audit requirements, both internal and external, are sufficiently met in order to have documented evidence of the security level within the organisation. In particular external audits required by external stakeholder and are relevant for the continued operations must be appropriately managed.

Penneo is obliged to allow authorities who in accordance with the legislation in force at any time have access to the facilities 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.