Disclosure Statement for TSA

Version history

Version	Date of release	Approved by (Title and name)	Comments
1.2	30.12.2024	Information Security Manager / Fredrik Lernevall	Improved reading. 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 TSA is the document required by European standard ETSI EN 319 421, related to the certification services offered by the Penneo as the Trust service provider (TSP).

In the following, the certification service is also referred to by "TSA service" (Time Stamp Authority).

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 TSA service 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. Electronic time-stamp types and usage

The Penneo’s qualified time stamping service follows Certificate Policy for TSA, Practice statement for TSA and Certification Practice Statement.

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

- ETSI EN 319 401
- ETSI EN 319 421
- ETSI EN 319 422

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. Time stamp content

Time stamp issued by Penneo’s TSA contains all information required by current legislation, including:

- time stamp serial number;
- time stamp algorithms - sha512withRSAandMGF1;
- the identifier of the certificate related to the public key of TSU;
- the date and time of the time-stamp;
- the accuracy of the time source compared to UTC.

Penneo's Time-stamp certification authority (RSA key at least 2048 bits, signature algorithm sha512withRSAandMGF1) is intended for issuing qualified certificates for electronic time stamp system.

2.2. Time Stamp usage - accuracy, limit

The qualified time-stamping service of Penneo is based on the use of TSP protocols on HTTP, defined in the regulation RFC 3161 'Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)'.
The accuracy of the qualified time-stamping of Penneo with respect to UTC is a second. The synchronisation service uses a fleet of satellite-connected and atomic reference clocks in each Region to deliver accurate current time readings of the Coordinated Universal Time (UTC) global standard through Network Time Protocol (NTP). The Provider's Time Sync Service automatically smooths any leap seconds that are added to UTC.

The accuracy is monitored and evaluated continuously.

The time verification will usually be executed automatically by the provider's application and always accordingly to the CPS, CP for TSA, Practice Statement and this document.

The electronic time-stamping services provided by Penneo are considered as automated services provided by Penneo's application (The Platform) and is in compliance with the current technical and legal regulation.

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. TSU public key certificate status

Relying parties may only use the time stamp certificates for the purposes described in the relying party agreements with Penneo and as described in the CPS, Terms and Conditions including necessary conditions for the Platform usage.

Under the correct verification of the electronic time-stamping certificates and compliance with this disclosure statement, the relying parties can trust the

provided information.

The Penneo's qualified electronic time-stamping services are not designed for use in unauthorized dangerous situations (that require fail-safe actions), such as nuclear facilities operations, navigation systems, air communications or weapon control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

If the relying parties are confident on an electronic signature related to a non-verified qualified electronic time-stamping, they will assume all risks from that action.

For relying parties is not possible to manipulate with Penneo's TSA infrastructure and perform any steps to destroy or misuse the application behaviour and proper functionality.

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 time stamp service.

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 TSA services based on applicable CPS and related CP for remote time stamp creation. 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 TSA 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 TSA 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 Certification Policy for Root CA;
  - Certificate Practice Statement for Subordinates CAs;
  - Trust Service Practice Statement with attachments for electronic signature, seal and time stamp;
- Certification Policies for:
  - remote and qualified electronic signature;
  - remote and qualified electronic seal;
  - remote and qualified electronic time stamp;
  - Certificate Practice Statement and Certification Policy for Root CA.
- 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

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 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Any complaint shall be sent to trustservice@penneo.com

10. TSA and repository licenses, trust marks, audit

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.