PS for Time Stamp Authority

Version history

Version	Valid from	Approved by (Title and name)	Comment
1.3	08.01.2026	COO / Christel Victoria Høst	General re-wording and alignment with standard terminology throughout the document for clarify and consistency. 1.6 updated accordingly. Details about the Penneo Platform's service and EULA for signers. 1.3.3 included possibility of different clients. 1.3.5 Elaboration of other participants.
1.2	26.11.2025	COO / Christel Victoria Høst	Minimum RSA key size changed from 2048 to 3072 for TSA certificate under 6.1.2.
1.1	30.12.2024	Information Security Manager / Fredrik Lernevall	Improved readability.
1.0	22.11.2022	Information Security Manager / Fredrik Lernevall	First release

Introduction

This document as an appendix to Penneo’s Trust Service Practice Statement with additional information about the procedures, activities and rules of this Practice Statement (hereinafter PS) that Penneo’s TSA Services (Time Stamp Authority

Services). Penneo, as a qualified trust service provider, implements the TSA Services exclusively for qualified remote certificates for time stamps.

Penneo's trust-building services are built and operated in accordance with eIDAS and applicable standards.

Penneo's TSA issues qualified electronic timestamps, which means messages of data which reliably link data in electronic form with the moment in time and which guarantee that the data (their fingerprint) in electronic form existed before the mentioned time.

The provision of the time stamp service is provided by one time-stamp unit (TSU). This unit has its own key and qualified certificate for the electronic time-stamp stamp. Penneo's TSA certificate (individual TSU) is issued by Penneo PKI.

1.1. Overview

The TSA Practice Statement (TSA PS) describes the facts related to the life cycle processes of the issued Certificates and follows the structure, the model of the valid standard RFC 3647, taking into account the valid technical standards and principles.

The document contains only additional information to relevant chapters found in the TSPS, hence why not all nine chapters from the TSPS are included:

Chapter 1 - provides 1) information about this document with a unique identifier, 2) description of the entities involved in the preparation, organisation and administration of the operation, 3) description of the implementation of Penneo's services and 4) defines the appropriate and prohibited use of certificates.

Chapter 3 - describes the process of identification and authentication of the subscriber, respectively certificate revocation or suspension.

Chapter 4 - describes the processes of the completeness and usage of issued time-stamp stamps certificates and the areas of audit and evaluation of the provided Services.

Chapter 6 - describes steps, requirements for life cycle of time-stamp stamp keys, rules and procedures of TSA.

Further descriptions are included in the Certificate Policy for Qualified Electronic Time Stamp certificate and internal documentation.

1.2. Document name and identification

Name of the document: Practice statement of Time-stamp authority.

1.3 TSA participants

1.3.1. TSA 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.

Time-stamp authority (TSA) services operated by Penneo:

- manages and covers the areas of creating and issuing time stamps;
- provides services in accordance with the eIDAS regulation and applicable standards.

1.3.2. Registration Authority

Registration authority is not used for purposes of this PS.

1.3.3. Subscribers

Penneo’s automated processes (hereinafter Platform) provide time stamps to subscribers who use Penneo's Platform Services of remote electronic signatures and sealing.

There are two types of subscribers for this service:

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

- Send an invitation to sign with a unique link to the SIC to each signer, via email or other appropriate client.

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

2. **Signers** (could be employees working on behalf of the Customer’s company, organization or other legal entity, employees of other Customers or other natural persons) - receive a request for signature via email or other appropriate client, containing a unique link to the Platform. Signers are not necessarily Penneo's customers but they enter an agreement with Penneo by accepting Penneo's End User License Agreement through the Signer Interaction Component before they sign.

Penneo is the owner of the TSA certificate and responsible for issuing qualified electronic time stamps as part of the Platform’s processes for remote electronic signatures and sealing.

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 time stamps of the signers’ signatures and document seals based on the CA’s hierarchy.

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

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 external data centre and the Platform is implemented to cloud solution. Cooperation is based on bilateral contracts between Penneo and parties.

1.3.5. Other participants

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

- Data centre services,
- Hardware suppliers,
- Software suppliers,
- Cloud solution provider,
- Time synchronisation service provider.

The suppliers' obligations and liabilities are described in the bilateral contracts with Penneo. Relevant parts are mentioned in Penneo's internal documentation.

Penneo is fully responsible for the activities of the contracted suppliers. Risk assessments are performed. In the case of a breach, an investigation is conducted. Based on the results, the supplier may incur a penalty or termination.

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

Penneo ensures availability of the Platform during the term of the Agreement - uptime of 99.9%.

Other participating entities may be:

- supervisory authorities
- law enforcement authorities.

1.4. TSA usage

This Practice Statement does not define any restriction for time stamp usage. The TSPS and CP for remote time stamp defines usability of time stamps if it is necessary.

1.5. Policy administration

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 1.5 of Trust Service Practice Statement.

1.6. Definition and acronyms

Definitions

Penneo’s CA Services	A set of certification authorities which is possible to use during electronic signature and electronic sealing - Root CA, subordinate CA, TimeStamp CA.
Penneo’s PKI Services	Penneo’s CA Services and qualified services for remote electronic signature and remote electronic sealing and stamping.
Certificate	A data message issued by a certification service provider combines data (code or public cryptographic keys that are used to verify an electronic signature) to verify signatures with the signer and allows to verify his/her identity.
Public Certificate Registry/Repository	An electronic registry where certificates and lists of revoked end-user certificates and service certificates are published. It is accessible according to the rules defined in the Certification Practice Statement or Certification Policy (CPS/CP) document.
Certificate policy (CP)	A set of rules that assess the applicability of certificates within individual groups and / or classes of applications in accordance with security requirements and is supported by Certification Practice Statement (CPS). It relates to the use of the certificate and to the use of data for the verification of the electronic signature of the holder for which the certificate has been issued.
Certificate Practice Statement (CPS)	It forms the framework of the rules set by the CP. They define in their procedures, provisions and

	regulations the requirements for all services entering the registration and certification process.
Certificate Revocation List /Repository(CRL)	List of expired certificates published by the Certification Authority to the Public Certificate Registry/repository (LDAP)
Electronic Signature	It expresses the general concept of signature, which is applied in an electronic environment. A wide range of means and technologies are used to generate this signature, including digital signatures and biometric methods.These are data in electronic form, which are attached to or logically connected to the data message and which enable the verification of the identity of the signer in relation to the data message.
Digital Signature	It is based on the use of cryptography (cryptosystems) with a public key. Currently, this term is used to refer to a special type of electronic signature. This type of electronic signature is used to verify the identity of the sender of the message or the person who signed the message. It is also used to verify that the message to which the digital signature was attached is not altered/modified.
Asymmetric cryptography - RSA	The principle of the method is that data encrypted by one of the keys can only be decrypted with knowledge of the other of the key pair and vice versa. One of the keys is called private, the other public. The RSA algorithm is used for asymmetric cryptography.
Private key	Data for creating a digital signature. Private part of an asymmetric key pair for cryptographic purposes. Used to sign and decrypt messages.
Public Key	Digital signature verification data. Public part of an asymmetric key pair for cryptographic purposes. Used to encrypt messages and verify digital signatures.

Registration Authority (RA)	Companies which are responsible for verifying the application for a certificate, identifying and authorizing the subscriber.
Electronic Seal	An electronic seal is a piece of data attached to an electronic document or other data, which ensures data origin and integrity.
Revoke the certificate	To terminate the certificate based on the responsible user's/manager’s request. The certificate cannot be renewed.
Suspension of the certificate	Suspend the certificate based on the responsible user's/manager’s request. Validity can be renewed.
Relying Party	An entity that relies on trust in a certificate and an electronic signature verified using that certificate.
Root CA	CA issuing certificates to Subordinate CA
OCSP responder	A server that provides public key status information in a certificate using OCSP protocol
Subordinate CA	CA issuing certificates to subscribers and relying services
TimeStamp CA	CA issuing certificates with time-stamp to subscribers

Acronyms

eIDAS	REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS 2 Regulation) provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.
PKI	Public Key Infrastructure - set of services (HW and SW) performing the all activities concerning to certificate life-cycle.

EJBCA	PrimeKey’s EJBCA is one of the longest running CA software projects, providing time-proven robustness and reliability. EJBCA is platform independent, and can easily be scaled out to match the needs of your PKI requirements, whether you're setting up a national eID, securing your industrial IOT platform or managing your own internal PKI. EJBCA covers all your needs - from certificate management, registration and enrolment to certificate validation.Software provided by PrimeKey. https://www.primekey.com/
LDAP	Lightweight Directory Access Protocol - Public Certificate Registry
OID	Object identifier (OID) - is an identifier mechanism used for naming objects based on a recognised standard by the International Telecommunication Union (ITU) and ISO/IEC that ensures globally unambiguous persistent names.
RA	Registration authority
IP	Identity providers
CA	certificate authority
TSA	Time stamp authority
UTC	Coordinated universal time
TSP	Trust service provider
HSM	Hardware security module
CRL	Certificate revocation list
CCID	Chip card interface device
DKEK	Device Key Encryption Key
UPS	Uninterruptible Power Supply
RQSCD	Remote Qualified Signature Creation Device Remote Qualified Seal Creation Device
SAM	Signature Activation Module
SAD	Signature Activation Data

SAP	Signature Activation Protocol
SIC	Signer Interaction Component
EULA	End User License Agreement

2. Publication and Repository Responsibilities

> This document does not bring any additional information to the Publication and repository responsibilities. For relevant information please see chapter 2 of Trust Service Practice Statement.

3. Identification and authentication

3.1. Naming

The naming scheme of Penneo's qualified trust services is approved by Penneo's managers and implemented by authorized Penneo employees.

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

Initial an identity verification and validation for certificates is performed through defined rules and procedures of Penneo and described in the internal documentation.

3.2.1. Method to prove possession of private key

Initial identity validation is specified in the relevant CP.

3.2.2. Authentication of organizational identity

Penneo is responsible for keys pair generation and issuing of the seal certificate and is the owner of the process.

3.2.3. Authentication of individual identity

Procedures are described in a specific CP for electronic seal. Penneo is responsible for the key generation process.

3.2.4. Non-verified subscriber information

Unverified information is described in a specific CP.

3.2.5. Validation of authority

Certificates of the subordinate CA for signature and seal are automatically implemented in the Platform's PKI services.

Validation of certification authority is fully automated process of the application developed by Penneo - The Platform and corresponding PKI services.

3.2.6. Criteria for interoperation

Penneo's CAs and PKI structure is created to allow subscribers to create remote qualified electronic signatures. It also enables the addition of qualified timestamps as part of the signature creation, and addition of Penneo's qualified electronic seal to the signed documents. Penneo's CAs and PKI do not implement connections with other CAs or other ways of interoperability.

3.3. Identification and authentication for re-key request

Penneo's CA services do not support the act of re-key. Identification and authentication is performed based on Key Management processes and under Penneo management.

3.3.1. Identification and authentication for routine re-key

See chapter 3.3.

3.3.2. Identification and authentication for re-key after revocation

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

3.4. Identification and authentication for revocation request

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. TSA operational requirements

4.1. TSA certificate application

4.1.1. Who can submit a certificate application

A certificate application for the issuance of the TSA certificate may be submitted by defined and authorized Penneo's employees.

4.1.2. Enrollment process and responsibilities

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

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

Penneo's authorized employees check the data and verify the written request with Penneo's management. They follow an internal written procedure for a key pair to be generated in the hardware security module (HSM), issue the certificate, and implement the certificate in Penneo's PKI service for use in the Platform's automated process.

The private key remains saved in the HSM, which is owned and managed by Penneo. It has been installed and is being operated according to the provider's documentation.

The keys use a suitable cryptographic algorithm as defined in the standard ETSI TS 119 312.

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 written request is evaluated by Penneo's management based on internal security procedures. The written request is either approved or rejected. Certificates are only issued with management approval 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. The certificate is issued during 3 working days after request.

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 authorized employees following internal written procedure. If all controls are met, the keys are generated securely in the HSM, where the certificate is also issued. The certificate issuance process is recorded.

The process of key pair generation and certificate issuance is managed and fully automated and performed in the HSM.

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

Issuance of the certificate is managed by internal procedures and the issued certificate is implemented in the Platform infrastructure.

The certificate and associated private key is used during the Platform's automated process of document processing (electronic signature, seal and time stamp).

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

Penneo's authorized employees create the certificate for the electronic timestamp and prepare it for automated processing in the Platform and cooperating PKI services. The process is approved by Penneo's management and defined steps are performed.

Subscribers, after all conditions of Penneo’s Platform and PKI services have been met, receive signed, sealed and time stamped documents. Subscribers can verify the validity of the certificate inside the document.

4.5. Key pair and certificate usage

The private key and certificate are issued by Penneo's authorized employees according to internal procedures. The private key is saved in the hardware security module which is owned and managed by Penneo as described in the standard ETISI TS 119 431-1.

Penneo's Platform ensures that the private key can only be used under Penneo's control, as part of the Platform's automated processes, whereby a Subscriber’s electronic signature is followed by electronic time-stamp confirming the date and time of the electronic signature.

4.6. Time stamp process

All processes relating to TS activities are part of the agreement between Penneo and subscribers.

4.6.1. Time Stamp request

The Platform is responsible for automated remote processes for electronic signature, time stamp and seal. The process is described in relevant CP.

If the process of the electronic signature, seal and time stamp of documents is completely and properly finished, the document is distributed to subscribers. The resulting document contains all signed information with the possibility to check and verify customers/signers, time stamps and seal.

4.6.2. Time for processing

Time for processing is not defined. Limitations can arise if the processes are interrupted or communication between subscribers and the Platform takes a longer time than validity of issued subscribers certificates for electronic signature. Subscribers have to start the process again from beginning.

4.6.2.1. Time service coordination

Penneo’s TSA service implements Amazon’s Time Sync Service, which 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 Amazon Time Sync Service automatically smooths any leap seconds that are added to UTC.

It meets the accuracy required by ETSI EN 319 421 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

Continuous monitoring of the accuracy is performed. If the accuracy is higher than a second, Penneo’s service does not issue time stamps.

4.6.3. Time stamp issuing and processing

Issuing of time stamps and processing is a fully automated process that is managed by tools and procedures within the Platform.

4.6.4. Time synchronization

The time stamp data (UTC) is obtained from the Provider’s Time Synchronization Services. The timestamp is provided with an electronic mark/seal of a specific TSU using the sha512withRSA Encryption algorithm (this undoubtedly guarantees this server for the accuracy of the information provided in the issued timestamp).

5. Facility, Management, and Operational Controls

> 📌 This document does not bring any additional information to the Facility, Management, and Operational Controls. For relevant information please see chapter 5 of Trust Service Practice Statement.

6. Technical Security Controls

6.1. Key pair generation and installation

Key pairs of CAs are generated and saved in secure cryptographic environment. Keys generation is under control of Penneo manager and it is part of initialization process. Secure cryptographic environment fulfills the requirements of standards EN 419 221-5 and are certified by Common Criteria level 5 for Root CA and by Common Criteria 4+ for subordinates CAs.

Generating of the Root CA keys - Key pair generation is performed in a computer centre’s dedicated area according to a pre-prepared internal initialization scenario.

Private keys of Subordinates CAs are saved in cryptographic hardware security module (HSM) according to a pre-prepared scenario under Penneo control.

Private keys for TSA certificates are generated in the same HSM as subordinates CAs. Private keys are saved in the HSM and used directly by the automated Platform processes for remote qualified electronic signature, seal and time stamp. Private keys and certificates are not downloaded to subscribers PCs.

6.1.1. Public key delivery

Key pairs are generated in the HSM module and public keys are issued and published within certificate. Subscriber can use certificate for electronic time stamp via automated process through web browser (the Platform). It is possible to download the certificate from Penneo web pages.

6.1.2. Key sizes

The size of keys for TSA certificate is minimally 3072 bits (RSA algorithm is used). Key usage purposes are defined in the certificate extension.

6.2. Private Key Protection

📌 This document does not bring any additional information to the chapters 6.2.1.-6.2.7. For relevant information please see chapter 6.2 of Trust Service Practice Statement.

6.2.8 Method of activating private key

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

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

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

A written protocol is created based on performed activities.

6.2.9 Method of deactivating private key

Deactivation of private keys of the TSA certificate stored in the hardware cryptographic module is performed with the direct personal participation of at least two Penneo employees authorized by Penneo’s management.

Written protocols are made of the deactivation.

First step before deactivation is to stop the Platform usage and realize 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.

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

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

6.3 Other aspects of key pair management

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.3 of Trust Service Practice Statement.

6.4. Activation data

This document does not bring any additional information to this chapter. For relevant information please see chapter 6.4 of Trust Service Practice Statement.

7. Certificate, CRL, and OCSP Profiles

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 7 of Trust Service Practice Statement.

8. Compliance Audit and other Assessments

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 8 of Trust Service Practice Statement.

9. Other Business and Legal Matters

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 8 of Trust Service Practice Statement.

Christel Victoria Høst

PENNEO A/S CVR: 35633766

Chief Operating Officer

Serial number: 66d16c3a-ebd4-4bba-beb5-6d4299861cb9

IP: 2.106.xxx.xxx

2026-01-08 05:26:37 UTC

Mit ID

Penneo document key: PFADX-RIMWY-P6OHK-2ZVWZ-407MI-EURCQ