PS for Time Stamp Authority

Version history

Version	Date	Approved by	Comment
1.0	22.11.2022	Information Security Manager / Fredrik Lernevall	First release

Introduction

This document as an appendix to the Trust Service Practice Statement supplements it with additional information and further specifies the procedures, activities and rules of specific Practice Statement (hereinafter PS) that the Penneo TSA Services (Services of TS Authority), as a qualified provider of trust-building services, implements in the provision of trust-building services and in issuing certificates (hereinafter also Services) exclusively for qualified remote certificates for time stamps.

Penneo's trust-building services are in accordance with eIDAS and EU regulation.

Penneo TSA issues qualified electronic timestamps, it 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 TSA certificate (individual TSU) is issued by the Penneo TS Qualified certification authority.

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 information about this document, describes the entities involved in the preparation, organization and administration of the operation and implementation of the Services.

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.

Other description is mentioned i the relevant Certificate Policy for time-stamp-stamps 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 company has implemented a two-tier CA structure. The self-signed certificates for Root CA and certificates for subordinate CAs. The Root CA issues certificates for Subordinate CAs - Time stamp certification authority and Certification Authority for electronic signature and 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 relevant legislation and technical standards.

1.3.2. Registration Authority

Registration authority Is not used for purposes of this PS. The all processes are managed by responsible Penneo employees.

1.3.3. Subscribers/customers

Penneo’s TSA Service issues time stamps to subscribers - natural, legal. The all activities are fully automated and performed via web browser (the Penneo Platform). The all TSA services are qualified.

1.3.4. Relying parties

Relying parties are entities (natural or legal) that rely on and use certificates issued by Penneo during fully automated and remote process of electronic signature verification.

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.

1.4. 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 CAs Services	A set of certification authorities which is possible to use during electronic signature an

	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	The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted on 23 July 2014 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, number base od object’s identification
RA	Registration authority
IP	Identity providers
CA	certificate authority
TSA	Time stamp authority
UTC	Coordinated universal time
TSP	Trust service provider
HSM	Hardware security modul
CRL	Certificate revocation list
CCID	Chip card interface device
DKEK	Device Key Encryption Key
UPS	Uninterruptible Power Supply

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

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

Anonymity or pseudonymity is not 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

The Platform is operated by Penneo, which has registered the name a trademark. Subscribers may use the Platform but shall respect the intellectual property rights.

The Subscriber is liable for compliance with the rights to the use of the Platform(s) and is explicitly made aware that the Platform(s) and the Penneo name, are protected by intellectual property rights, and the Subscriber is liable for any misuse of such.

3.2. Initial identity validation

Initial an identity verification and validation for seal 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 to the Penneo PKI services cooperating with the Platform.

Validation of certification authority is full 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 remote qualified electronic time stamp, signature and sealing services. It does not implement connections with other CA or other ways of interoperability.

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 a TSA certificate may be submitted by defined and responsible Penneo’s employees or managers.

For Penneo’s TSA, all process is managed by internal rules approved by Penneo manager.

4.1.2. Enrollment process and responsibilities

The certificate application processes start with Penneo’s CEO’s written request. All information about OID and common names (including name of this CP) has to be prepared in advance and included in the request.

It is the responsibility of Penneo's responsible employee to become acquainted with the certificate processes and to provide complete, accurate and true data.

Penneo's manager or Penneo's responsible employee checks and verifies mentioned data according to written request and initiates the key generation process.

Penneo's responsible employees has to perform activities to publish the certificate and implement the certificate to Penneo's PKI services for automated processes.

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

4.1.3. Time to process certificate applications

The time for issuing Penneo seal service's certificates is during 3 working days after request. The all is based on internal procedures.

4.2. TSA Certificate issuance

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

4.3. TSA Certificate acceptance

For TSA certificates of Penneo PKI services is verification and acceptance of certificates managed by internal procedures during and after generation.

The process of a the keys pair generating, certificate issuing and certificate acceptance is managed and fully automated and performed in the secure hardware cryptographic module.

4.4. Key pair and certificate usage

The Penneo’s responsible employees carry out steps according to internal regulations and publish the certificate for approved usage in the Platform’s remote automated processes. Subscriber’s electronic signature is followed by electronic time-stamp confirming the date and time of the electronic signature.

4.5. Time stamp process

The all processes concerning to TS activities are part of the agreement between Penneo and subscribers.

4.5.1. 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 subscribers can see the document with signatures, time stamps and seals.

After processing the document is saved to secure database for following activities - verification or law purposes.

4.5.2. 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.

4.5.2.1. Time service coordination

This 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 Amazon Time Sync Service automatically smooths any leap seconds that are added to UTC.

It meets the accuracy required by ETSI.

Continuous monitoring of the accuracy is performed. If the accuracy is higher than a second, server does not issue time stamps.

4.5.3. Time stamp issuing and proccessing

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

4.5.4. 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

The key pair generation for creating of a remote electronic certificates for time stamps is performed in a hardware cryptographic module, which is under the control of Penneo and fulfils the requirements of Common Criteria EAL 4+.

Cryptographic modules provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection and key, data and application encryption.

Written protocol about TSA keys generation is created and signed by responsible Penneo employees and participants.

Time stamp certificate parameters are defined before the initialization process and the private key is implemented to hardware cryptographic modules during initialization. Parameters meet requirements of eIDAS and technical standards.

6.1.1. Public key delivery

Key pairs are generated in the hardware cryptographic 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 it from Penneo web pages.

6.1.2. Key sizes

The size of keys for TSA certificate is minimally 2048 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

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 responsible Penneo employees 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 private key is performed with the direct personal participation of at least two Penneo employees authorized by Penneo’s management and performed according to a precisely determined procedure.

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.

6.3 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.