# PS for Remote Electronic Seal

**Version history**

| Version | Date of release | Approved by (Title and name) | Comments |
|---|---|---|---|
| 1.0 | 22.11.2022 | Information Security Manager / Fredrik Lernevall | First release |
| | | | |

# 1. Introduction

This document as an appendix to the Trust Service Practice Satement supplements it with additional information and further specifies the procedures, activities and rules of specific services (hereinafter Practice Statement - PS) that the Penneo implements in the provision of remote trust-building services (hereinafter as Services) and in issuing certificates (hereinafter also Platform) exclusively for qualified remote electronic seal. Penneo's trust-building services are in accordance with eIDAS and EU regulation.
The service is provided to Customers on the basis of the particular Certificate Policy for qualified remote electronic seal (hereinafter CP) which describes trustworthy system of Penneo's PKI services and is defined by RFC 3647 standard.

## 1.1. Overview

The Practice Statement for qualified remote electronic seal (PS) describes the facts related to the life cycle processes of the issued time stamps 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. 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 of Services life cycle, from the Platform for issuance, the processes of issuing certificates, confirmation and approval of certificates, including notification of certificate issuance.

**Chapter 6** - describes the technical side of security of public and private key generation, cryptographic standards, algorithms they are used.

## 1.2. Name and document identification

Name of the document:

Practice Statement of qualified remote electronic seal (RSA algorithm)

## 1.3 Trust services participants

### 1.3.1. Certification Authority for remote electronic signature and seal

Penneo is a qualified provider of trust services under the eIDAS Regulation:

- Issues certificates for remote and qualified electronic signature and seal;
- operates and manages trusted systems to support the Penneo's electronic signature platform (hereinafter the Platform), based on applicable standards;
- establishes and carries out web application to support the Platform;
- uses the services of third parties in a scope necessary in its activities - the computer centre, cloud solution and Amazon time synchronization services.

### 1.3.2. Service Participants

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.

Registration Authorities/Identity Providers - providing identification and verification of subscribers, issuing subscribers ID identifier that is used for remote automated processes of The Platform. The agreement between Penneo and subscribers is described in Terms and Conditions.

PKI services are implemented in the Computer center and use technology of cloud service provider.

### 1.3.3. Subscribers

The Subscribers (legal company) use certificates for sealing process within Penneo's Platform and use the Penneo Platform services through internet connection and web pages remotely.

### 1.3.4. Relying parties

Relying parties are entities (natural or legal) that rely on and use qualified electronic seal issued by Penneo in their activities. More is possible to see in related CP for electronic seal.

### 1.3.5. Other participants

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

## 1.4. Service usage

### 1.4.1. Appropriate usage

Qualified seal services under this Practice Statement resp. related Certificate policy may be used in processes for qualified electronic seal only in accordance with applicable law and legal requirements.

### 1.4.2. Prohibited certificate uses.

Unauthorized use of seal services means any use that is in conflict with the appropriate usage and the CP under which it was issued.

## 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. Service life-cycle operational requirements

## 4.1. Seal certificate application

### 4.1.1. Who can submit a certificate application

A certificate application for the issuance of a Seal certificate may be submitted by defined and responsible Penneo’s employees or managers.

For Penneo’s seal certificates 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. Seal Certificate issuance

The process of the key pair generating and issuing the certificate is fully automated and is implemented in a secure cryptographic module.

All processes of generation and issuing of certificate for qualified electronic seal are managed by responsible Penneo's employees.

## 4.3. Seal Certificate acceptance

For seal certificates of Penneo PKI services is verification and acceptance of certificates managed by internal procedures during and after generation. The process is approved and managed by Penneo manager and defined steps are performed.

## 4.4. Key pair and certificate usage

The Penneo's responsible employees carry out steps according to internal regulations and steps and publish the certificate for approved usage in the Platform's remote automated processes.

### 4.4.1. Seal service agreement

The Agreement provides the subscriber's access to the Platform, enabling the subscriber to access agreed services.

The Agreement applies to delivery of the Platform and additional services from Penneo to the subscriber unless it has been expressly derogated from or modified by another written agreement and it can be established with certainty that the intention was to derogate from this agreement.

The purpose of the Agreement is to lay down the conditions for the delivery of the Platform and the Seal services to the subscriber.

### 4.4.2. Seal service activation

Seal Service activation is carried out by remote automatic process - The Platform usage cooperating with PKI Services:

- unambiguous identification of subscribers at the places of the RA/IP and issuance of a unique subscriber's ID as the input for automated process via the internet Platform;

- using the subscriber’s ID for remote and automated process via internet Platform for the process of the private and public keys generation and certificate issuing. The subscriber confirms own data and agrees with conditions and necessary rules included to so named Declaration and Consent inside the internet Platform;
- if all subscribers sign the document:
  - PKI services cooperating with the Platform send request for electronic seal;
  - the document is sealed and saved to the internal database.

### 4.4.3. Seal service creation

The Seal service is part of automated remote process of the Platform and PKI services. The document is signed by particular signers and prepared for sealing. Remote sealing process is activated, verifies that all signatures are present and creates the electronic seal.

The seal is part of the signed document.

# 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

> 📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.1 of Trust Service Practice Statement.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

> 📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2 of Trust Service Practice Statement.

## 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.

## 6.5 Computer security controls

> 📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.5 of Trust Service Practice Statement.

## 6.6 Life cycle technical controls

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.6 of Trust Service Practice Statement.

## 6.7. Network security controls

Penneo's root CA is not accessible to subscribers and the status is off-line. The rest of Penneo’s services, which is through subordinate CA’s are accessible via the internet but protected through numerous security measures like network segmentation to ensure that the Platform is logically separated other resources is access is restricted to only authorised persons.

The same security controls are applied on all systems within one zone.

Trust Service components must be kept in a separate zone and especially system critical components for the TSP (such as Root CA) are kept in (one or more) secured zone.

All connections that are not needed for the service operated in the production environment must be deactivated / blocked, i.e. a deny by default policy must be applied. This also means that access and communications between zones for TSP operations are restricted to only those necessary.

Communication between trustworthy systems is running only through trusted channels. These channels are isolated physically from other communication channels. These measures provide guaranteed identification of their endpoints and protect the channel data against modification or disclosure.

Transfer of data between registration authorithies are performed via encrypted communication between Penneo’s services is through secure internet channel (protocol https).

# 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.