PS for Remote Electronic Signature

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 Statement (TSPS) 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 signature based on ETSI TS 119 431-1 standard.
Penneo's trust-building services are designed and operated to comply with eIDAS and EU regulation.
The service is provided to Customers on the basis of the particular Certificate Policy for remote electronic signature (hereinafter CP) which describes trustworthy system of Penneo's PKI services and is defined by RFC 3647 standard.

1.1. Overview

The document describes the facts related to the life cycle processes of the issued certificates and follows the structure of the standard RFC 3647, taking into account the valid technical standards and principles.

Technical requests and detailed information about this problematic are described in internal documentation.

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 with uniques identification, describes the entities involved in the preparation, organization and administration of the operation and implementation of the PKI Services. Defines the appropriate use of certificates.

Chapter 3 - describes the process of identification and authentication of the subscriber for a certificate, respectively certificate revocation or suspension. Describes methods for prove possession of a subscriber's private keys, the role of trademarks, and the uniqueness of names. Shortly deals with re-key procedures.

Chapter 4 - describes the processes of the completeness of certificate life cycle, from the Platform for issuance, the processes of issuing certificates, confirmation and approval of certificates, including notification of certificate issuance. Chapter solves the process of requesting certificate revocation, processes and services related to verification of certificate acceptance, usage of certificate and following steps and possibility of renewal, re-key and modification of certificate etc.

Chapter 6 - describes the technical side of security of public and private key generation, cryptographic standards, algorithms they are used. Describes methods for activating and deactivating private keys. It solves the issue of computer and network security, their principles and required control mechanisms.

1.2. Document name and identification

Name and Identification of the document:

Practice Statement for remote electronic signature (algorithm RSA).

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. Subscribers

Penneo’s automated process provides qualified remote certificates to identified subscribers (customers/signers) via a Registration authority/Identity provider and uses Penneo's Platform services and application for remote qualified electronic signature.

The application of remote electronic signature is developed by Penneo and presented to subscribers (customers/signers) via web browser. Details of agreement between Penneo and the customer are described in internal document - Terms and Conditions.

The Services of remote qualified electronic signature use several actors:

- **Customers** - means a company, organisation or other legal entity, on behalf of which a 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.
  - They are identified in Registration Authorities (RA) (see below chapter Definition and Abbreviations) and a subscriber ID is issued for them;
  - The Penneo Platform can verified theirs subscriber ID;
  - Identified a verified customers prepare documents for remote electronic signature and send to signers invitations (via e-mail notification) to sign the document.
- **Signers** (could be other Customers) - are notified by link inside e-mail message, initializes process of remote electronic signing. Signers are not necessarily Penneo's customers but Penneo have an agreement with them, since they accept the terms before they sign.
  - They are identified in Registration Authorities (RA) and a subscriber ID is issued for them;

    - The Penneo Platform can verified theirs subscriber ID;
    - The Signer uses the link inside e-mail message and can display the text of document. Approves start of electronic signature of the document. Before signing the signer has to be verified.
    - The Signer uses subscriber ID and is identified and authenticated via remote communication to RA. If the verification process is successful the Signer’s electronic token (e_token) is sent to the Platform for following processes.
    - Text of Declaration and consent is displayed to the Signer for approval. The Signer confirms Declaration and consent and personal data which is implemented to the Signer’s certificate. Confirms intention to sign the document.
    - The electronic signature process is finished and the signed and sealed document is sent to all signers.
    - Signers can be employee working on behalf the company, organization or other legal entity;
- **Penneo** as trustworthy provider through the Platform:
    - operates and is responsible for the Platform availability including the Public Key Infrastructure (PKI) services;
    - is responsible for a customers/signer verification and processing of remote electronic signature, seal and time stamps;
    - is qualified provider for provision of qualified and remote services;
    - uses external parties for the Platform implementation.

1.3.3. Registration authorities

Registration authorities (RA) are external companies (third parties) and their activities, among others are:

- to perform physical identification of subscribers on the RA contact points;
- to perform identification of legal company on the RA contact points;
- to save subscribers identification information to their databases;

- to issue unique subscriber’s digital identifier (ID) for subscriber verification in Penneo’s solution (the Platform);
- based on Penneo’s remote request provide needed subscribers personal information which are implemented to certificates.

List of possible RA is published in CP for electronic signature.

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 remote electronic signature of a the signer's based on the CA’s hierarchy.

Relying parties are informed about Penneo’s activities in the Platform for remote electronic signatures of documents.

1.3.5. Other participants

Penneo performs certain activities on a contractual basis and is fully responsible for the activities of their contracted suppliers. These commercial legal relations are regulated by bilateral contracts between:

- Penneo and Registration authorities in the role of Identity Providers,
- Penneo and the Computer center,
- Penneo and hardware and software suppliers,
- Penneo and cloud solution provider,
- Penneo and Amazon time synchronization services.

These suppliers are obliged to follow the relevant parts of the contract and mentioned Penneo’s internal documentation.

In the case of breaches the risk assessment should be performed. Based on the results penalty or termination can occur.

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 availabilty to the Platform during the term of the Agreement - uptime of 99.9%.

Other participating entities may be:

- supervisory authorities or law enforcement authorities.

1.4. Certificate usage

1.4.1. Appropriate certificates uses

Subscribers certificates may be used for remote electronic signature and electronic seal of documents in accordance with legal requirements. The application of certificates is included in the Certificate.

1.4.2. Prohibited certificate uses.

Unauthorized use of a certificate means any use of the Certificate that is in conflict with the type of the Certificate 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

Naming of subscribers are depend on a subscriber’s ID issued in contact with RA/IP.

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

Uniqueness of names is created in the process of a subscriber registering and creating a unique identifier (subscriber ID) in RA/IP contact points. Based on subscriber’s verification in the Penneo's digital signature platform (hereinafter Platform) an electronic token (e_token) is sent from particular RA/IP which contains subscribers personal information. The information is inserted to subscriber’s 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 process of identity verification and validation is performed through defined rules and procedures of so named Identity Providers which perform procedures as Registration Authorities (RA/IP) for the Penneo Platform.

RAs/IPs implement process of the subscriber identification and validation and issue electronic token (e_token) that Penneo has integrated with its Platform.

3.2.1. Method to prove possession of private key

Private key ownership is realized through a complex process:

- unambiguous identification of subscribers in an RA/IP contact points and issuance of a unique subscriber’s ID Identifier as the input for automated process via Penneo’s Platform;
- usage of the subscriber’s ID Identifier for the processes of verification of the subscriber via communication between the Platform and particular RA/IP. Before generation of keys and issuing of a certificate the subscriber has to confirm displayed personal data and information included to the Declaration and consent.
- personal data (e_token) and signature activation data is sent to the Platform after successful confirmation;
- the Platform implements data and via internal processes cooperates with PKI services and generates key pairs and a certificate. The subscriber can use the private key and the certificate for remote and automated process of remote qualified electronic signature, seal and time-stamp via the Penneo Platform.

3.2.2. Authentication of organizational identity

Authentication of organizational identity is performed by when the electronic identification has been set up from an organization and a particular RA/IP through applicable RA/IP procesdures. The RA/IP has to confirm an organizational identity. A RA/IP uses processes and means supporting unambiguous identification and authentication before issuing ID Identifier. An organizational entity is included to the name structure and published in a certificate together with subscriber’s identity.

3.2.3. Authentication of individual identity

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 before issuing of a subscriber’s ID identifier. Without issued subscriber’s ID is not possible to start remote and automated process of the Platform for remote and qualified electronic signature.

3.2.4. Non-verified subscriber information

For better information about non-verified subscriber’s information see web pages of a particular RA/IP.

3.2.5. Validation of authority

Penneo’s PKI services use subscriber’s ID identifier and corresponding subscribers electronic token (e_token) for generation of keys pair and issuing a certificate as an input for remote automated process of electronic signature via internet connection.

Validation of Penneo's CA is performed through defined application processes through CA’s tree verification.

The certificates of the subordinated CAs are implemented to the Platform’s application processes which perform activities for electronic signature and seal based on Penneo’s CA tree.

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. Certificate/signing key life-cycle operational requirements

4.1. Certificate application

4.1.1. Who can submit a certificate application

A certificate application may be submitted automatically via internet connection by a subscriber (natural/legal) with subscriber’s ID identifier issued by a particular RA/IP.

4.1.2. Enrollment process and responsibilities

A RA/IP has to verify subscriber’s data completeness and accuracy and issue unique subscriber’s ID identifier.

It is the responsibility of the RA/IP to maintain up-to-date information of the subscriber's identity. A particular RA/IP provides adequate and accurate data to the Penneo Platform.

The certificate is issued based on subscriber’s ID verification during internet communication between the Penneo Platform (via subscriber’s web browser) and particular RA/IP. The process is fully automated:

- a subscriber has to be verified and authenticated;
- a subscriber has to confirm conditions inside Declaration and consent and personal data displayed before signature;
- a subscriber has to express intention to sign the document.

4.2. Certificate application processing

Processing of subscriber’s certificate request is divided into several parts:

- The subscriber (customer/signer) personally ask for the unique subscriber ID identifier in a particular RA/IP contact points - soo also chapter 3.2. The exact procedure is described in particular RA/IP procedures;
- The subscriber (customer) logs in the Penneo Platform and prepares documents for signatures. The subscriber’s web browser is used;
- After documents are prepared and implemented to the Platform, an e-mail is sent to the subscriber (signer). The e-mail contains a link to documents.
- The subscriber (signer) displays documents and can read them. After the subscriber agrees with text of documents the subscriber confirms intention to sign documents. All is performed via the browser.
- Web application displays list of RAs/IPs and waits for the subscriber choice of particular RA/IP.
- The subscriber uses subscriber’s ID and performs identification and authentication to the Penneo Platform. Communication between Penneo Platform and particular RA/IP takes place with result of the subscriber’s validity and authenticity.
- If verification is valid and the subscriber is identified, a particular RA/IP sends so named electronic e_token which contains subscriber’s personal data as a input to a certificate and the Platform processes;
- The Platform displays Declaration and consent and subscriber’s personal data for confirmation;
- If the subscriber confirms necessary information, generation of keys pair is carried out, a subscriber’s certificate is issued and documents are electronically signed;

- Penneo’s application sends to the subscriber e-mail message with information that documents are signed and attaches the documents. The subscriber can verify signature, time stamp and seal.
- Documents which are returned by Penneo Platform after finishing will be in the format PAdES-PDF.

The same process is performed for all subscribers which are on the list of e-mail recipients receiving the notification. After all signers have signed a given document an electronic seal is added to the documents to protect the origin and integrity of the data in the document.

4.2.1. Performing identification and authentication

The subscriber’s identity is verified in RA/IP contact points. Subscriber’s ID identifier is issued and passed to the subscriber.

Identification and authentication og subscribers:

- The subscriber (customer) Identification and authentication is performed by the subscriber that prepares documents for signature.
- The subscriber (signer) clicks on link inside of e-mail and confirms intention to sign the document. Communication between Penneo Platform and particular RA/IP starts. The result is confirmation of the subscriber’s identity. At the same time RA/IP sends personal data (e_token) in defined structure to the Penneo Platform.

If the identification and authentication phases are successful the subscriber can continue in following phases of remote electronic signature.

4.2.2. Signing key generation

Generation of a signing key is realized and managed in the secure hardware cryptographic module. This module is published on the list of EU of this modules which is regularly monitored.

The all activities of the key pair generation and usage is carried out in the Platform (inside cryptographic modules) under Penneo’s controls.

4.2.3. Approval or rejection of certificate application

The process of certificate rejection or approval is based on the appropriate identification of the subscriber. If the subscriber is incorrectly identified in a particular RA/IP or/and invalid authentication does not perform correctly, the request is rejected by the Penneo Platform.

The Platform checks validity of the subscriber and verifies subscriber’s confirmation (Declaration and consent).

A certificate is issued if identifications and verifications are successful.

4.2.4. Time to process certificate applications

The time for issuing certificates of subscribers is immediately after fulfilling all automated phases for remote verifying the subscriber’s identity and subscriber’s approval of necessary requirements.

4.2.5. eID means linking

The key pairs generation for the subscribers is performed through an automated and complex process with participation of Registration Authorities in the role of the Identity Provider.

The subscriber identity is verified via the Platform remotely on RA/IP based on electronic object identifier (subscriber eID) issued by RA/IP after the subscriber’s proper identification and authentication on the RA/IP business places.

The customer/signer is asked for subscriber ID with possibility to choose the particular RA/IP that confirms his/her identity. After successful identity confirmation the customer/signer receives electronic token (e_token) that is used for the remote Platform automated processes.

The result of e_token implementation is the signer key pair generation, issuing of the certificate and final document with customer/signer signature, time stamp and seal.

The process of the customer’s/signer’s e_token implementation is fully automated and takes place via the web application and web browser.

4.2.6. eID means provisions

Before creation of remote electronic signature, the subscriber's identification and authentication is performed through web communication with the particular RA/IP. After

successful verification of subscriber’s eID the Platform creates e_token by automated process.

This e_token is used for key pairs generation and completion of requirements that are necessary for remote electronic signature, time stamp and seal.

The subscriber’s private key is saved inside of the cryptographic module that is under Penneo's control.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

The process of key pair generation and the certificate issuing is completely automated and is implemented in a secure hardware cryptographic module remotely.

After verifying of the subscriber’s identity during the identification and authentication phase in the Platform, the connection to a RA/IP is created. Through this internet connection, the Platform receives an e_token used for following phases of Penneo’s services via internet. The process takes place automatically, by Penneo's software implementing steps of identity verification, verification of the correctness of the entered data and approval of requirements within remote Penneo Platform.

After all conditions are met, keys are generated remotely in the hardware cryptographic module and the subscriber’s certificate is issued based on sent data. The subscriber can continue by following phases of electronic signature creating.

Creation of certificates and activities of CA is fully automatic process and are performed in cryptographic modules.

4.3.2. Certificate linking

Certificate linking with the subscriber's private key is performed through the Platform.

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

Penneo’s PKI services issue subscriber certificates and store them to the public registry.

Signing information is sent to the subscriber via the Penneo Platform via the internet. The subscriber can start the electronic signature and sealing on documents.

The process is automated. Subscribers provide consent for the processing of all subsequent steps in the Platform (from key generation to the certificate issuing and electronic signature).

Creation of certificates and activities of CA is completely automated process and are performed in cryptographic modules.

4.4. Certificate acceptance

The CA services implement certificate information and uses it in the next steps of the certificate processing. Acceptance of CAs certificates and activities of CAs is automated process and are performed in cryptographic modules.

4.4.1. Conduct constituting certificate acceptance

The subscriber confirms the intention to perform electronic signature in the Platform prior to the processing of key generation, certificate issuing and electronic signature.

4.4.2. Publication of certificate by the CA

Subscribers certificates are generated and stored in the public registry.

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

The services of key generation, certificate issuance and notification that the certificate is provided to the subscriber is based on an automated process of the Platform and CA services.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

The subscriber’s private key and certificate usage is a one time process. The private key is deleted after the electronic signature is created. The certificate is published to the registry.

The subscriber’s responsibility are:

- usage of the private key and certificate according to processes mentioned in this CP;
- usage of the private key and certificate according to relating legal purposes only;

- be informed in advance about electronic signature behavior and necessary steps have to be fulfilled.

Subscribers have to inform Penneo's contact persons (see TSPS 1.5.2) immediately, if:

- some suspicion exists about misuse of a private key or inappropriate behaviour of the Platform;
- data in the certificate is not complete or accurate. If the information is inaccurate, subscriber has to send the information to Penneo contact points and arrange a new registration process.

4.5.1.1. Signature activation

The Customer:

- is verified in the Platform and prepares one or more documents for signature. Process is managed by Web application;
- defines the list of signers necessary for document signature and sends invitation to signers via e-mail client.
- Signers use link included in the e-mail application and via Web can view text of the document (WISYWIS).
- After getting acquainted with the text of document can start signing of the document.
- Signers is obliged to identify and authenticate themself, based on the Subscriber ID, through communication with RA
- If the authentication is performing without problems the processes follows by:
    - generation of key pair in the cryptographic module and
    - the document is signed and time stamped.
- In the case that more than one signers are asked for signature the Platfrom collects all signatures and after the last signature the document is sealed.
- Final document information after signatures completion is send via e-mail to signers.

The documents which are returned by Penneo after the process in the Platform is finalized, will be in the format PAdES-PDF. The returned files contain all signature

certificates, are locked for editing and are, at the time of return to the Subscriber and Third Party, activated for long-term storage.

4.5.1.2. Signing key deletion

Penneo does not keep customer’s signing private key. Subscriber’s private key is deleted after the signature by the Platform and native cryptographic module resources.

4.5.1.3. Signing key backup and recovery

The signing key backup and recovery is not provided by Penneo. The keys are for single use only.

4.5.2. Relying party public key and certificate usage

A relying party may be obligated to rely on certificates mentioned in this CP which are consistent with applicable certificate content.

Relaying parties are recommended to download relating CA certificates from Penneo's web pages and verify content of certificates - minimally common name, fingerprint and validity before usage of subscribers certificates - and verify fingerprints of these certificates. They have to verify if the CA is qualified for trustworthy services and evaluate whether the certificate issued by a subordinate certification authority pursuant to this policy is suitable for the purpose for which the certificate was issued.

4.5.3.Signature creation application services component technical requirements

The Platform’s front end is the application running in the subscriber’s browser. Subscriber through the Web sends requests for the Penneo Services and interacts with the Platform.

Interaction is split into 4 logical flows:

1. Authentication flow.
2. User signing flow.
3. Validation flow.
4. Sealing flow.

Subscriber interacts in:

- Authentication flow.
- User Signing Flow.

Before the customer/signer can sign any document, identification and authentication must be successfully performed and valid subscriber authorization e_token has to be sent to the Platform.

Only validated signed data can be stored in the database. This is also confirmation that the signing process has been done correctly and no manipulation with the signed data happened.

The document is finalized (signed and sealed) when all customers/signers sign the document. The resulting PDF document contains all signed information with possibility to check and verify costumers/signers, time stamps and seal and it is distributed to all signatories.

4.5.4. AdES digital signature creation

Digital signature is created inside the cryptographic module.

4.6. Certificate renewal

A subscriber’s certificate renewal is not provided by Penneo's CAs services. The CAs issues always a new certificate.

4.6.1. Conditions under which certificate renewal takes place

See chapter 4.6.

4.6.2. Who may request certificate renewal

See chapter 4.6.

4.6.3. A CA or RA’s procedure to process renewal request

See chapter 4.6.

4.6.4. Notification of the certificate to the subscriber

See chapter 4.6.

4.6.5. Conduct constituting acceptance of the certificate

See chapter 4.6.

4.6.6. Publication of the certificate by the CA

See chapter 4.6.

4.6.7. Notification of certificate issuance by the CA to other entities

See chapter 4.6.

4.7. Certificate re-key

Penneo's CA services create new subscriber certificates in the case that the Platform processes are not finished or crashed. After analysis and correction the CA always issues a new subscriber certificate.

4.7.1. Conditions under which certificate re-key can or must takes place

The process of re-key can start if the Penneo Platform does not not finish all activities or interrupts processing (unavailability of connection, accidental events, not common behavior of the Platform, freezing or other mistakes during processes of connections and signing). After corrections new subscribers certificates are issued.

4.7.2. Who may request certificate re-key

The process is the same as during common Platform usage. See chapter 4.1.

4.7.3. A CA or RA's procedure to process re-key request

See chapter 4.7.2.

4.7.4. Notification of the certificate to the subscriber

See chapter 4.7.2.

4.7.5. Conduct constituting acceptance of the certificate

See chapter 4.7.2.

4.7.6. Publication of the certificate by the CA

See chapter 4.7.2.

4.7.7. Notification of certificate issuance by the CA to other entities

See chapter 4.7.2.

4.8. Certificate modification

The CA always issues a new certificate based on previous identification and authentication of subscribers (with subscriber ID usage) in particular RA/IP.

4.8.1. Conditions under which certificate modification can take place

See chapter 4.8.

4.8.2. Who may request certificate modification

See chapter 4.8.

4.8.3. A CA or RA’s procedure to process modification rerquest

See chapter 4.8.

4.8.4. Notification of the certificate to the subscriber

See chapter 4.8.

4.8.5. Conduct constituting acceptance of the certificate

See chapter 4.8.

4.8.6. Publication of the certificate by the CA

See chapter 4.8.

4.8.7. Notification of certificate issuance by the CA to other entities

See chapter 4.8.

4.9. Certificate revocation and suspension

A subscriber’s certificate is issued for one time process only and for time limited period. The certificate revocation and suspension is not supported and a request to revoke the certificate in the future is not supported.

For CAs is described in particular CP for seal and time stamp certificates.

4.9.1. Circumstances for revocation

see Chapter 4.9.

4.9.2. Who can request revocation

see Chapter 4.9.

4.9.3. Procedure for revocation request

see Chapter 4.9.

4.9.4. Revocation request grace period

see Chapter 4.9.

4.9.5. Time within which CA must process the revocation request

see Chapter 4.9.

4.9.6. Revocation checking requirement for relying parties

see Chapter 4.9.

4.9.7. CRL issuance frequency

The Root CA of Penneo's services issues CRL once a half a year with validity time one year.

Subordinate CAs issue the CRL every 12 hours, with time validity 24 hours.

4.9.8. Maximum latency for CRLs

The CRL for electronic signature and seal is always issued no more than 12 hours after the issuance of the previous CRL.

4.9.9. On-line revocation/status checking availability

OCSP is not used.

4.9.10. On-line revocation checking requirements

OCSP is not used.

4.9.11. Other forms of revocation advertisement available

Certificates for electronic signature are issued with time limited period. Other forms are not supported.

4.9.12. Special requirements re-key compromise

Special requirements re-key compromise are not supported.

4.9.13. Circumstances for suspension

Penneo’s CA services do not support suspension of subscribers certificates for electronic signature.

4.9.14. Who can request suspension

Penneo’s CA services do not support suspension of subscribers certificates for electronic signature.

4.9.15. Procedure for suspension request

Penneo’s CA services do not support suspension of subscribers certificates for electronic signature.

4.9.16. Limits on suspension period

Penneo’s CA services do not support suspension of subscribers certificates for electronic signature.

4.10. Certificate status services

4.10.1. Operational characteristics

Certificates issued by Subordinated CA’s are published and available on Penneo's web pages.

CRLs are regularly issued and published on Penneo's web pages.

Certificates contain information about a subscriber’s personal information and the certificate usage.

All processes of a certificate status verification is performed by the Platform and is fully automated and complex process without interruption.

4.10.2. Service availability

Services of Penneo's PKI are available 24 hours a day, 7 days a week. CRLs are available on addresses defined in certificates.

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 is 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.

4.10.3. Optional features

CRLs are available 7 days a week, 24 hours.

4.11. End of subscription

Penneo's CA, issuing certificates for subscribers (physical or legal), performs qualified services and is responsible for performing all promised activities mentioned inside CPS, TSPS and/or this CP for the time period of certificates are valid (for the period of validity of the last issued Certificate).

Subscriber's certificates have short validity time and process of validity verification is managed by internal Platform procedures.

Conditions and rules are described in internal key management documentation.

Subscription period for access and usage of the Platform is defined by the agreement between Penneo and subscribers.

Either Party may terminate the Agreement at a written notice of 3 months to expire at the end of the subscription period. If the Agreement is not terminated at the latest 3 months before the expiry of the subscription period, this gives rise to a new subscription period of 12 months.

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

6.1.1 Key pair generation

📌 This document does not bring any additional information to the Key pair generation. For relevant information please see chapter 6.1.1 of Trust Service Practice Statement.

6.1.2 Private key delivery to subscriber

Private keys are saved in the cryptographic module. Everything is performed by remote and automated way, nothing is saved on subscriber’s PC.

6.1.3 Public key delivery to certificate issuer

Not relevant. For subscribers, the key pair generated and stored in the secure cryptographic module.

A subscriber can use a certificate via remote automated process through web browser.

6.1.4 CA public key delivery to relying parties

The certificates are part of signed documents and it is possible to verify them by standard mechanisms implemented to PDF documents.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2.1 of Trust Service Practice Statement.

6.2.2 Private key (n out of m) multi-person control

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2.2 of Trust Service Practice Statement.

6.2.3 Private key escrow

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2.3 of Trust Service Practice Statement.

6.2.4 Private key backup

Subscribers private key has no backup. They are generated and processed only once.

6.2.5 Private key archival

Private key for subscribers are not archived. They are generated and processed only once. For next signature has to be a new key pair generated.

6.2.6 Private key transfer into or from a cryptographic module

It is not relevant for subscribers.

6.2.7 Private key storage on cryptographic module

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.2.7 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.

6.2.9 Method of deactivating private key

Deactivation of subscriber’s private key is managed by automated Penneo Platform. If signing process ends correctly and documents are electronically signed the subscriber’s private key is deleted by the Penneo Platform.

6.2.10 Method of destroying private key

Destroying of subscriber’s private key is managed by Penneo Platform. The private key is used only once.

6.3 Other aspects of key pair management

6.3.1 Public key archival

📌 This document does not bring any additional information to this chapter. For relevant information please see chapter 6.3.1 of Trust Service Practice Statement.

6.3.2 Certificate operational periods and key pair usage periods

Subscriber certificate operational period is defined in the certificate .

There is no difference between operational and key pair usage period. The last subscriber’s certificate will be issued in date prior to expiration of the CA’s certificate.

Validity time of private key and corresponding public key located in certificates is the same.

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.