POINTSHARP

Certificate Policy and Certification Practice Statement

PoSC Net iD SweID

Secure Cloud
Net iD

Digitally signed by PsPT
Date: 2023.10.02 14:30:09 +02'00'

Classification:	Public
Publication No.:	PSC-Rd22-01
Document version:	1.2
Document status:	Final
Date:	29 Sep 2023

Table of Contents

1 INTRODUCTION

1.1 Overview

Pointsharp AB manages the Pointsharp Secure Cloud Net iD SweID (Net iD SweID) public key infrastructure (PKI) that includes a service that issues subscriber certificates compliant to the Swedish eID Assurance Framework ("Tillitsramverk för Svensk e-legitimation" issued by DIGG, Myndigheten för digital förvaltning (the Swedish Agency for Digital Government), with identity assurance 3 (LoA3) and 4 (LoA4) (hereinafter called "The Service").

Within The Service, certificates are issued by customer organizations (RAs) to individuals (subscribers) with ties to the customer organization, for instance employees, consultants, students and contractors. The subscribers must have a Swedish personal identity number ("personnummer") or a Swedish coordination number ("styrkt samordningsnummer"), and must be at least 16 years old.
RA organizations can be private as well as public organizations having a customer agreement with Pointsharp.

Pointsharp offers The Service to organizations that have signed a Pointsharp Secure Cloud Net iD SweID Customer Agreement ("Kundavtal för Pointsharp Secure Cloud Net iD SweID"; Customer Agreement) including a Pointsharp Secure Cloud Net iD SweID Data Protection Agreement ("Personuppgiftsbiträdesavtal för Pointsharp Secure Cloud Net iD SweID"; DPA). The Customer Agreement refers to this combined Certificate Policy and Certification Practice Statement (CP and CPS) and to Pointsharp Secure Cloud Net iD SweID RA Trust Framework ("Pointsharp Secure Cloud Net iD SweID Tillitsramverk för RA"), and will stipulate the rights and obligations for each part in the agreement. All customers (RAs) must state their compliance to The RA Trust Framework in the Pointsharp Secure Cloud Net iD SweID RA Declaration of Compliance ("Pointsharp Secure Cloud Net iD SweID Tillitsdeklaration för RA") relating to applicable sections in The RA Trust Framework. The RA Declaration of Compliance needs to be approved by the Pointsharp service Policy Team (PsPT) before the start of the RA operations. The RA Declaration of Compliance and RA operations will be subject to an initial review by PsPT, before the RA organization is approved to connect to The Service.

Individuals, organizations and functions that rely on Net iD SweID certificates are referred to as a relying party. All revocation control services, that is, services for OSCP and revocation lists, are provided for free to relying parties.

1.1.1 Certificate Policy

This document defines the combined Certificate Policy (CP) and Certification Practice Statement (CPS) addressing the provisioning and life cycle management of the Net iD SweID certificates issued within The Service.
This includes information on how the issuing of certificates complies with applicable parts of the stipulations in the Swedish eID Assurance Framework.
The Service is operated by Pointsharp.

The CAs complying with this CP and CPS will sign and issue certificates to physical persons with a Swedish personal identity number or a Swedish coordination number.

This CP and CPS is published and periodically reviewed under the authority of PsPT. The CP and CPS is published at: https://repository.pointsharpsecurecloud.com.

Subscriber certificates are issued by the subordinate issuing CAs:

- Pointsharp SweID 4 CA vX
- Pointsharp SweID 3 CA vX
- Pointsharp SweID Mobile 3 CA vX

The number following "SweID" in the CA names represents the level of assurance and the "X" represents a version number in sequence from "1" and upwards.

Subordinate issuing CAs are issued by the Root CA "Pointsharp SweID Root CA v1".

No organizations other than Pointsharp are allowed to operate a certificate issuing service relating to this CP and CPS.

This CP and CPS complies with the Internet Engineering Task Force (IETF) publications:

1. RFC 3647 for Certificate Policy and Certification Practice Statement construction,
2. RFC 2119 Key words for use in RFCs to Indicate Requirement Levels.

This CP and CPS is subject to compliance audits in accordance with section 8.

1.1.2 Scope of applicability

This CP and CPS covers the issuing of LoA3 and LoA4 certificates within The Service to subscribers with a professional relationship to organizations that are customers of The Service (RAs).

This CP and CPS is primarily intended for the following parties:

- Personnel in the PoSC Operational Team.
- Subcontractors used by The Service and processing centers that operate under the terms of this CP and CPS.
- Customer organizations (RAs) that operate under the terms of this CP and CPS and The RA Trust Framework.
- Relying parties who need to understand how much trust to place in the certificates issued by The Service. For most cases, this means verifying an authentication or a signature made with a LoA3 or LoA4 subscriber certificate.
- Auditors that conduct audits of different parts of The Service.

1.2 Document name and identification

The Object Identifiers (OIDs) for The Service are derived thus:

Pointsharp AB	{iso (1) member-body (2) se (752) pointsharp (179)} OID: 1.2.752.179

Pointsharp Secure Cloud documentation	{posc (100)} OID: 1.2.752.179.100
Trust Frameworks	{trustframeworks (1)} OID: 1.2.752.179.100.1
CA Policies	{capolicies (2)} OID: 1.2.752.179.100.2

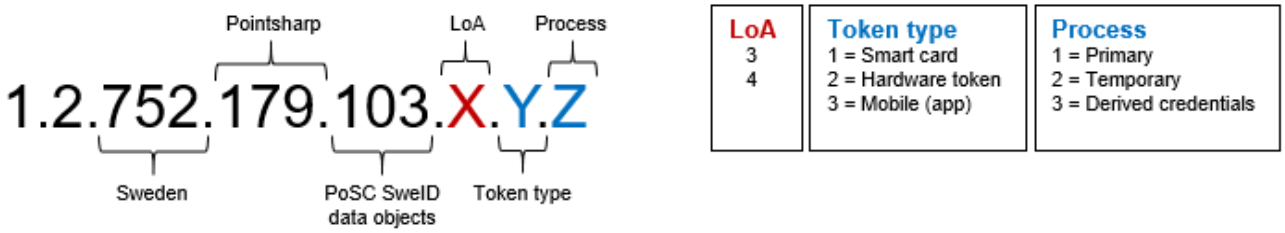
In order to provide discrete OIDs for The RA Trust Framework, and this CP and CPS, the following OIDs have been determined to identify the formal releases of these documents:

Pointsharp Secure Cloud Net iD SweID Tillitsramverk för RA	{sweid-frwrk (3)} OID: 1.2.752.179.100.1.3
Pointsharp Secure Cloud Net iD SweID Certificate Policy and Certification Practice Statement (this document)	{sweid-cp-cps (3)} OID: 1.2.752.179.100.2.3

All subscriber certificates issued by The Service will have a policy identifier that makes it possible to identify the certificate issuance process and how the associated private keys are secured:

1. LoA: the identity assurance level,
2. Token type: how the private keys is protected,
3. Process: the process used during issuance.

The logic of the OIDs used in the policy identifier is described in figure 1.1.



1 Figure 1.1: Logic for the OID in the policy identifier.

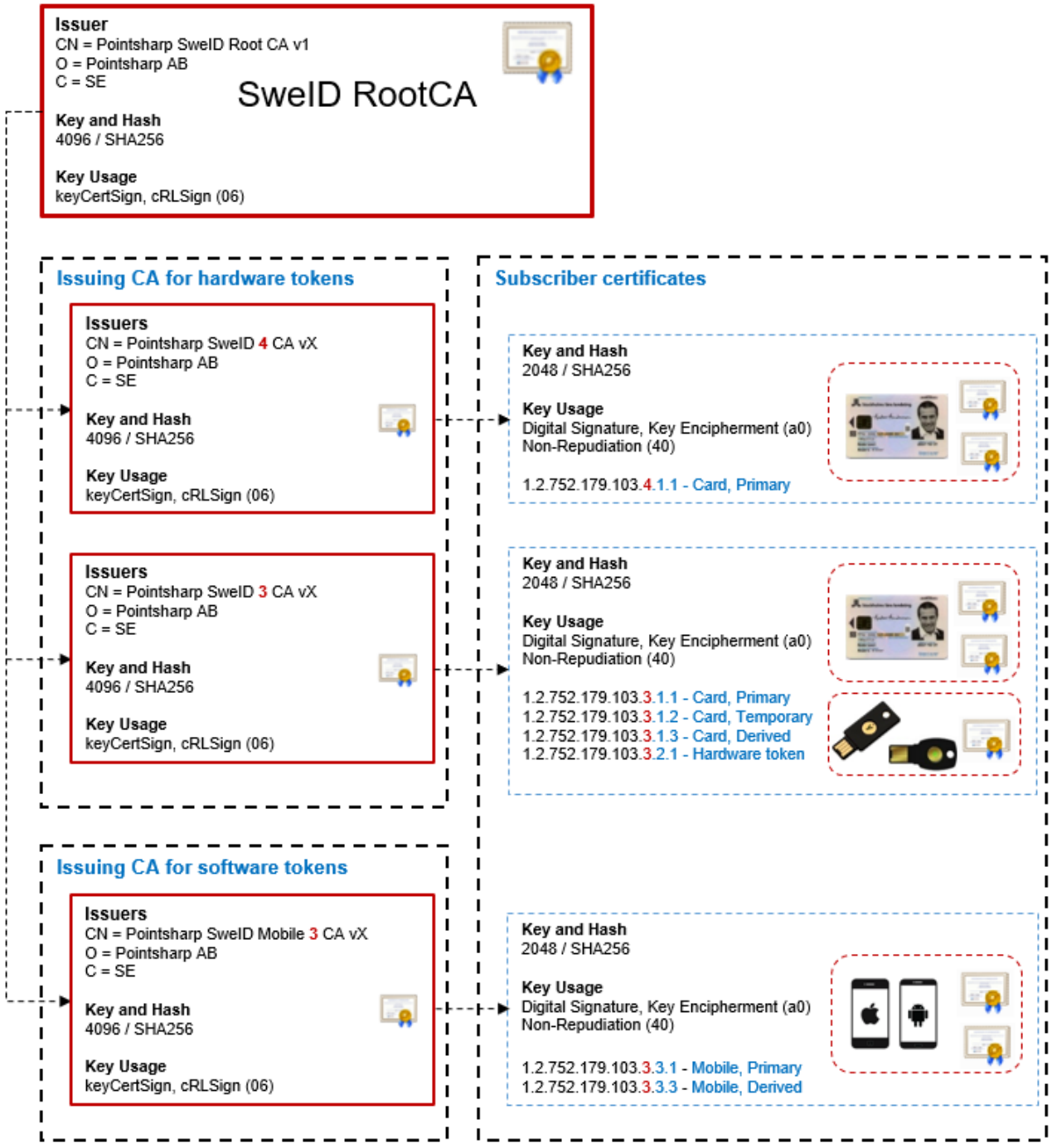
CAs used in The Service issue subscriber certificates with the following policy identifier OIDs:

- Pointsharp SweID 4 CA vX:
  - 1.2.752.179.103.4.1.1
- Pointsharp SweID 3 CA vX:
  - 1.2.752.179.103.3.1.1
  - 1.2.752.179.103.3.1.2
  - 1.2.752.179.103.3.1.3
  - 1.2.752.179.103.3.2.1

- Pointsharp SweID Mobile 3 CA vX:
  - 1.2.752.179.103.3.3.1
  - 1.2.752.179.103.3.3.3

For more information regarding CAs, subscriber certificates, and the valid OIDs in the policy identifier of the subscriber certificates, see figure 1.2 below.

This CP and CPS must apply to any entity asserting any of the OIDs listed.



2 Figure 1.2: CAs, subscriber certificates, and valid OIDs in the policy identifiers.

The "X" in the name of the issuing CAs represents a number for the CA version starting on "1".

1.3 PKI participants

This section describes the entities relevant to the administration and operation of The Service.

All of the participating entities must undertake what is stated in this CP and CPS. This CP and CPS applies to Pointsharp, RAs, Pointsharp subcontractors, subscribers, relying parties and auditors.

1.3.1 Certification authorities

The term Certification Authority (CA) refers to entities authorized to issue public key certificates and includes two subcategories of issuers:

- Root Certification Authority. The Net iD SweID Root CA acts as the root for all subordinate CAs that are part of the Net iD SweID CA hierarchy. The Root CA used within The Service can only issue subordinate CA certificates.
- Subordinate Issuing Certification Authorities. The set of Net iD SweID subordinate Issuing CAs issue subscriber certificates based on the approved certificate profiles governed by PsPT.

Pointsharp manages The Service and the CAs that are the scope of this CP and CPS. The Service is responsible for managing the certificate life cycle of CAs and subscriber certificates signed by those CAs. This includes:

- creating and signing of certificates binding subscribers, CA personnel, and RA personnel to their public encryption keys;
- providing certificate status through OCSP responders; and
- providing certificate status through certificate revocation lists (CRLs).

The Root CA and issuing CAs used within The Service are shown in figure 1.2 above.

1.3.2 Registration Authorities

Registration Authorities (RAs) refer to entities that perform enrollment procedures for subscriber certificate applications and initiates or pass along revocation requests for certificates, on behalf of a CA. This can either be the organization or the person ultimately responsible for certificate issuance and revocation within an organization.

Organizations responsible for RA functions are:

- Pointsharp acting as central RA for The Service with access to all RA domains, hereinafter referred to as "Service RA" in this CP and CPS.
- Customer organizations acting as RAs in their own RA domain.

Individuals assigned to an RA role must have shown suitability for the role and be appointed by a representative with the appropriate mandate in their RA domain. An RA domain consists of one customer organization.
The organization name of the RA domain is included in all certificates issued under its domain.

All RAs must adhere to The RA Trust Framework and the terms in the Customer Agreement. Each RA is accountable for the fulfillment of all stipulations of The RA Trust Framework within their RA domain and must operate in accordance with their RA Declaration of Compliance approved by PsPT. PsPT verifies the RAs compliance to The RA Trust Framework and applicable sections of this CP and CPS upon initial application and then through random reviews or if found necessary by PsPT.

1.3.3 Subscribers

Subscribers under The Service include all end entities of certificates issued by a CA listed in section 1.3.1.

According to this CP and CPS, only a physical person with a Swedish personal identity number or a Swedish coordination number can be a subscriber. The subscriber must be of 16 years age or older to qualify for a certificate.

Subscribers must agree to The Service's Subscriber Terms and Conditions before receiving a certificate.

1.3.4 Relying parties

A relying party may be either an RA organization with a valid customer agreement for The Service or any other organization, person, application, or device that relies on subscriber certificates issued by The Service.
Organizations taking part as relying parties in DIGG's framework for Prepaid e-identification ("Förbetald e-legitimering") must have a valid agreement with DIGG.

Relying parties must check the validity of a certificate with the appropriate OCSP service or the appropriate revocation list prior to relying on information featured in a certificate.

All subscriber certificates contain a policy identifier that provides some additional information to relying parties about the specific process used to issue a subscriber certificate and how the private keys related to the certificate are stored, see section 1.2.

1.3.5 Other participants

1.3.5.1 Auditors

The Service will require the services of other organizations, such as compliance auditors. Depending on the scope of the audit, such auditors are appointed by the Pointsharp Board or by PsPT.

1.3.5.2 Processing centers

Processing centers are entities that are not a CA but they participate in the issuance process of certificates. Pointsharp will use card manufacturers as such entities.

1.4 Certificate usage

1.4.1 Appropriate Certificate Uses

Certificates issued under this CP and CPS may be used for the purposes designated in the Key usage and Extended key usage fields of the certificate.
However, the sensitivity of the information processed or protected by a certificate varies greatly, and each relying party must evaluate the application environment and associated risks before deciding on whether to use a certificate issued under this CP and CPS.

Certificates are normally used by subscribers to sign and encrypt information, authenticate themselves to applications (client authentication), and encrypt communication (such as TLS). Certificates can be used for other purposes, provided that a relying party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, the Swedish eID Assurance Framework, this CP and CPS, or any agreements with subscribers.

1.4.1.1 Subscriber certificate key usages

Key usages used for Subscriber certificates are:

- digitalSignature and keyEncipherment:
  Certificates with this combination of key usages are used to identify the subscriber stated in the subject of the certificate when used for authentication by the subscriber. It can also be used for encryption purposes.
- nonRepudiation (contentCommitment):
  Certificates with this key usage are used to verify the signature of the Subscriber stated in the signature certificate when used for signing by the subscriber.

Extended key usages that may be used in subscriber certificates are:

- clientAuthentication (1.3.6.1.5.5.7.3.2)
- emailProtection (1.3.6.1.5.5.7.3.4)
- smartCardLogon (1.3.6.1.4.1.311.20.2.2)

1.4.1.2 CA certificate key usages

Key usages used for Root CA certificates and CA certificates are:

- keyCertSignUsed by CAs to sign subscriber certificates and by Root CA to sign CA certificates.
- cRLSignUsed by CAs to sign subscriber certificate revocation lists and by Root CA for off-line signing of CA certificate revocation lists.

1.4.2 Prohibited certificate uses

Certificates do not attest to the good behavior of the certificate subjects (subscribers). They must not be taken to guarantee that the subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with.

Certificates issued under this CP and CPS may not be used by any subscribers in relation to any of the following:

1. where prohibited by any laws, be they national, European or international
2. where the usage does not correspond to the Key Usage or the Extended Key Usage stated in the certificate
3. certificates issued to identify physical persons must not be used for functions

There are no provisions within this CP and CPS for cross-certification or other forms of recognition or usage of certificates issued under this CP and CPS by or with certificates issued by other Certificate Authorities as or under any other PKIs.

1.5 Policy administration

1.5.1 Organization administering the document

The "Responsible authority":
Pointsharp service Policy Team
Phone: +46 8 601 23 00
E-mail: pspt@pointsharp.com

1.5.2 Contact person

See section 1.5.1

1.5.3 Person determining CPS suitability for the policy

The "Responsible authority" cited in section 1.5.1 is the administrative entity responsible for determining the suitability of this CP and CPS.

1.5.4 CP approval procedures

Each formal release of this CP and CPS requires approval by PsPT whose signature will be applied to an electronic version of it. On the effective date all previous versions will become redundant. PsPT will preserve records of all past versions.

1.6 Definitions and acronyms

Unless alternative definitions, meanings or interpretations are assigned in Appendix A of this CP and CPS, the definitions in RFC 3647 apply.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

PsPT is responsible for making information regarding The Service available according to the following:

- **Regulatory documentation and CA certificates**
  This CP and CPS, The RA Trust Framework, CA certificates, certificate and CRL specifications, issuance processes, and related documents are published at https://repository.pointsharpsecurecloud.com.

- **Audit information concerning parties involved in the operations of the PoSC service and RAs' Declaration of Compliance**
  This information is not publicly available but will be stored internally at Pointsharp.
- **Revocation information**
  For entities that wants to validate certificates issued by The Service, revocation information is freely available as follows:
  - CRL & ARL: http://crl.pointsharpsecurecloud.com/<CA common name>.crl, for example: http://crl.pointsharpsecurecloud.com/pointsharpsweid3cav1.crl
  - OCSP: http://ocsp.pointsharpsecurecloud.com/
  - AIA: http://aia.pointsharpsecurecloud.com/<CA common name>.cer, for example: http://aia.pointsharpsecurecloud.com/pointsharpsweid3cav1.cer.

2.2 Publication of certification information

The following information is available according to section 2.1:

1. This CP and CPS
2. Issued CA certificates
3. Revocation information is publicly available via certificate revocation list (CRL), CRL for CA certificates (ARL), online certificate status protocol (OCSP), and authority information access (AIA).
   All published CRLs and ARLs, hereinafter both are referred to as CRLs, provides all available revocation information at the time of publication. Revocation information is only available for certificates issued by the CA that the revocation list in question is intended for. Revocation information given via the OCSP service corresponds to the most current revocation information available in The Service.

No information regarding the content of issued subscriber certificates, nor the actual certificates, will be published and publicly available.

2.3 Time or frequency of publication

All information, including changes in the regulatory documentation, is published promptly after it is decided within The Service. Changes that may affect subscribers, RAs, and relying parties will be announced well in advance at the repository before the change is implemented in the regulatory documentation. Contact persons at all RAs are also informed. Regulatory documentation is reviewed by PsPT when necessary or at least every 12 months.

The OCSP service is available 24 hours a day, all days of the year, except when there is planned maintenance or other factors beyond Pointsharp's control.

Revocation information of issued subscriber certificates will be updated promptly or at least within one hour from an accepted certificate revocation request.

2.4 Access controls on repositories

Regulatory documentation, CA certificates, AIAs, CRLs, and OCSP services are provided publicly with unrestricted read access as described in section 2.1.

Logical and physical controls have been implemented to prevent unauthorized modifications of information in the repositories.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Net iD SweID CAs issue certificates with a non-null Subject Distinguished Name (DN) that complies with ITU X.500 standards.

Every subscriber's identity is registered along with a set of attributes.

Subscriber certificates issued related to this CP and CPS are only issued to individuals with either a Swedish personal identity number ("personnummer") or a Swedish coordination number ("styrkt samordningsnummer").

Identities and attributes are verified by involved RAs and the SPAR service (Statens PersonAdressRegister; Swedish Tax Authority's national register with individuals holding a Swedish personal identity number or a Swedish coordination number, including official names of individuals and their home addresses) before a certificate is issued.

Each subscriber will also be provided with an additional identification number that is unique within The Service, a "Subsriber PoSC ID". This PoSC ID is created automatically by The Service.

The composition of names for different types of certificates is defined in the certificate specifications that are published on the repository, https://repository.pointsharpsecurecloud.com.

3.1.2 Distinguished names

Distinguished names in certificates issued by The Service are ensured to be unique by means of a unique identifier.

For subscriber authentication certificates the unique identifier is contained within the certificate as Subject serial number and serves as the general identification attribute for the subscriber. The unique identifier must contain the subscriber's Swedish personal identity number or Swedish coordination number.
The Subscriber PoSC ID that is provided by The Service is also included in the certificate as the title attribute (T) of Subject DN.

For subscriber signature certificates only the Subscriber PoSC ID is included as a unique identifier in the certificate (in the title attribute).

In addition to the unique identifier, the Subject DN of the certificates also contains other verified information about the subscriber:

Subscriber information	Attribute	Verifying method
Name (given names, middle name and surname)	G & SN	The official name of the subscriber according to SPAR.
Common name (first name and surname)	CN	A "friendly name" of the subscriber. The first name and surname of the subscriber according to SPAR.
Organization name	O	The RA domain. The official organization name of the RA having a relationship with the subscriber and being responsible for issuing subscriber certificates under their domain. Verified by the CA.
Organizational Unit	OU	The VAT identification number of the RA organization. Verified by the CA.
Organizational Unit	OU	An organizational unit within the RA organization related to the subscriber. According to the records of the RA organization, if available.
Locality	L	The main locality of the RA organization. Verified by the CA.
Country	C	The country where the RA organization has its main business. Verified by the CA.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers are not allowed to use anonymous or pseudonymous names.

3.1.4 Rules for interpreting various name forms

Distinguished Names in certificates must be formed and interpreted using X.500 standards and ASN.1 syntax.

3.1.5 Uniqueness of names

The uniqueness is ensured as described in section 3.1.2.

3.1.6 Recognition, authentication, and role of trademarks

RAs (customers) must not use names that infringe upon the intellectual property rights of another entity. Explicitly, no certificates may include any trademark, nor the identifying marks of any entity other than the RA issuing the request.

At the time of the Customer Agreement, Pointsharp makes controls to ensure that the RA organization has applied intellectual property rights to the organization name and domain names used in the certificates. The customer is responsible to inform Pointsharp of any events that result in changes of official organization name, ownership of domain names, or other intellectual property rights that can have an effect on the Customer Agreement.

Pointsharp will not be required to determine whether an organization has intellectual property rights to the names in a customer agreement or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, or trademark.
PsPT is entitled, without liability to any customer agreements, to suspend any certificates issued by an RA organization because of such disputes.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

3.2.1.1 Smart cards personalized at card manufacturer

Depending on the smart card used, the subscriber's private keys are generated in one of two ways at the card manufacturer appointed by Pointsharp:

- Keys are generated in the chip of the smart card (onboard key generation).
- Keys are generated in a hardware module and then transferred securely to the smart card.

The key generation is done in the same production process where initialization and personalization of the card take place. Signed PKCS#10 requests are made by the personalization systems at the card manufacturer site and are sent to the CA systems of The Service. The systems of The Service validate the signature of the RA certificate used making the certificate requests and validate the signature of the requests.
The private keys of the RA certificate used by the personalization system are stored on a smart card or other hardware token and all certificate requests can be traced to the individual responsible for the request by logs at the card manufacturer.

After the validation of signatures, the certificates are issued by the appropriate CA and returned to the card manufacturer to be stored in the corresponding smart card. The personalized card is then distributed by registered mail to the RA that has requested issuing of the smart card with the corresponding certificate under its domain.
Personalized smart cards and activation codes, associated with the private keys of smart cards, are delivered to the subscribers via separate channels.
For LoA4 certificates a code letter with PINs and PUK is distributed to the subscriber's home address.
For LoA3 certificates the PUK are distributed to the central management system and PINs are chosen by the subscriber when receiving the smart card.

3.2.1.2 Certificates issued at RA

If the CA does not generate the key pair of the Subject but it is generated in the RA organization, either by an RA Officer or by the subscriber, the CA will verify the

possession of the private key by verifying the electronic signature included in the certificate request.

3.2.2 Authentication of organization identity

Before a Customer Agreement is signed with a new RA organization, wanting to use The Service, a number of controls are made by the PoSC Operational Team to verify the suitability and credibility of the organization to act as an RA of The Service.

3.2.2.1 Organization authentication

Depending on organization type, information from the Swedish Companies Registration Office and/or the Swedish Central Bureau of Statistics is used to verify the legal registration of the organization, that it is active in its registered location and has a physical address.

3.2.2.2 Economic status

For non-public organizations, the economic status of the organization is verified with UC (Upplysningscentralen). If any irregularities are found the organization can be denied a Customer Agreement.

3.2.2.3 Operational existence

A check is made to verify that the organization exists and is operational, also see sections above.

3.2.2.4 Verification of authorization

To verify that the authorized contact person, according to the Sign-up preparation form, is working at the named customer organization, a phone call is made to the official switchboard telephone number and a request is made to speak with the named contact person.

3.2.2.5 Domain authentication

The organization's ownership of domain names is verified by:

- Sending a message via https://www.domain-contact.org/ requesting contact with the domain owner.
- Checking information at Internetstiftelsen (.se and .nu domains).
- Checking information at whois.net (other top domains).

3.2.3 Authentication of individual identity

For any application of a subscriber certificate, the subscriber's identity will be verified in accordance with the issuance routines of The Service and The RA Trust Framework. When issuing certificates with identity assurance level LoA3 and LoA4 the subscriber must be identified with a valid identity document, approved by The Service, both at the time of application and when receiving the smart card or hardware token with the certificates and corresponding private keys.

In the case of issuing LoA3 subscriber certificates through the use of derived identities, the identity of the subscriber is verified by demanding the subscriber to authenticate with an X.509 certificate issued with the corresponding level of assurance or higher, that is, LoA3 or LoA4. The private keys corresponding to the subscriber certificate used to authenticate must be protected within a smart card or other hardware token. Only issuers trusted by The Service can be used for derived issuance. The issuer may be another CA within The Service or a third party issuer that is compliant to the Swedish eID Assurance Framework. The same unique identifier will be used for the subject in the derived authentication certificate as is included in the subject serialnumber attribute of the certificate used for authentication. The unique identifier will not be included in the signature certificate but the certificate is linked to the unique identifier of the subject via the Subcriber PoSC ID.

All subscribers that receive a certificate must have a relationship with the RA organization issuing the certificate under its domain. For all identity assurance levels, the professional correlation of each subscriber must be asserted by means of manual or automated control in local employment registers or in other directories used by the RA.

At the registration of a subscriber in The Service, before certificates are issued, The Service automatically verifies the Swedish personal identity number or the coordination number of the subscriber with the records of the SPAR service. During the verification, information regarding the official name of the subscriber are retrieved from the SPAR service.

Before issuing LoA4 certificates the Swedish personal identity number or the coordination number of the subscriber is used to retrieve the official home address of the subscriber.

3.2.4 Non-verified subscriber information

Non-verified subscriber information is not allowed.

3.2.5 Validation of authority

The Service must validate the authority of an entity requesting any type of certificate issuance by verifying that they are the requesting CA or RA Officer. Authentication will rely on LoA4 or LoA3 certificates issued according to the Swedish eID Assurance Framework.

For issuing of LoA4 certificates, only LoA4 certificates issued by "Pointsharp SweID 4 CA vX" are trusted.

For issuing of LoA3 certificates, certificates issued for assurance level 3 or higher may be trusted. In addition to relying on certificates issued within The Service, Pointsharp can also choose to rely on certificates issued by any other Issuer compliant to the Swedish eID Assurance Framework.

RA Officers with LoA4 certificates are able to issue and manage LoA4 and LoA3 certificates.
RA Officers with LoA3 certificates are able to issue and manage LoA3 certificates.

All CA Officers and CA Administrators within the PoSC Operational Team will use certificates issued via LoA4 issuing processes for management of The Service.

3.2.6 Criteria for interoperation

Interoperation is not allowed.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Routine re-key is not supported.
No specific routine exists for the renewal of a certificate issued by The Service. Renewal of keys and certificates are ordered and delivered in the same way as new certificates meaning, a new validation of the subscriber will be executed.

3.3.2 Identification and authentication for re-key after revocation

See section 3.3.1.

3.4 Identification and authentication for revocation request

Revocation procedures ensure, prior to any revocation of any certificate, that the revocation has in fact been requested by either:

1. The certificate subscriber,
2. An RA Officer or authorized applicant within the subscribers organization, or
3. Authorized personnel in The PoSC Operational Team

If key compromise is suspected for a private key associated with an issued certificate, the certificate is allowed to be revoked even if the identification and authentication requirements cannot be completely fulfilled.

Acceptable procedures for authenticating a revocation request of a subscriber certificate are as follows:

Revocation requester	Method of request	Identification method
Subscriber	Self-administration portal	Authentication by mutual TLS, and an additional encryption layer, with a certificate issued by a CA that is trusted by The Service.
	Telephone call	Call to the RA helpdesk that asks control questions that proves that the caller has knowledge about the certificate to be revoked.

Revocation requester	Method of request	Identification method
RA Officer, authorized applicant, or other authorized representative within an RA domain	Administration portal	Authentication by mutual TLS, and an additional encryption layer, with a certificate issued by a CA that is trusted by The Service.
	Telephone call	Call to the RA helpdesk that asks control questions that proves that the caller has knowledge about the certificate to be revoked.
RA Officer or other authorized representative within PoSC Operational Team	Administration portal	Authentication by mutual TLS, and an additional encryption layer, with a certificate issued by a CA that is trusted by The Service.
	Telephone call	Call to The Service helpdesk that asks control questions that proves that the caller has knowledge about the certificate to be revoked.
Processing center	Secured communications	Requests revocation of certificates in case of production errors through secured communication with PoSC Operational Team.

4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Entities within The Service who may submit certificate applications:

- subscribers who are the subject of the certificate and is an employee of, or has another relationship with, an RA organization
- authorized representatives of an RA organization
- RA Officers or authorized applicants of an RA organization
- CA Officers and other operational staff at Pointsharp, subcontractors, or processing center

4.1.2 Enrollment process and responsibilities

RA Officers or CA Officers are responsible for validating the identity of each applicant (subscriber). All validations must be performed in accordance with the LoA4 and LoA3

issuance processes of The Service and The RA Trust Framework prior to the authorization and issuance of a certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All applicants must be identified according to the requirements stipulated in section 3.2.3. Authentication and identification must be done in accordance with the issuance processes within The Service and The RA Trust Framework. The issuance process may vary depending on the requested certificate's level of assurance and other circumstances. All applications will be digitally signed ensuring that all requirements of The Service have been fulfilled.

4.2.2 Approval or rejection of certificate applications

CA Officers and RA Officers within The Service will authorize and approve all applications if the application can be verified in accordance with section 3.2.3.
CA Officers and RA Officers must reject all applications that cannot be verified in accordance with section 3.2.3.

4.2.3 Time to process certificate application

CA Officers and RA Officers must begin to process certificate applications within a reasonable time.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The issuance of a certificate means that the issuing certificate authority accepts the application and the subscriber information that the subscriber has declared.

Certificates are generated and issued after a CA Officer, RA Officer, or other authorized applicant has verified the application and fulfilled all control routines.
To be able to trace a certificate application back to the individual that made the application, all certificate applications are digitally signed by the CA Officer, RA Officer, or other authorized applicant.

Prior to the subscriber certificate issuance process, all official personal data of the subscriber will be verified and updated with information from the Swedish Tax Agency by using the SPAR service.

4.3.2 Notification to subject by the CA of issuance of certificate

The Service issues certificates to subscribers upon request. A notification is sent to the subscriber that a certificate has been issued or is available for issuance.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The acceptance of the terms and conditions for use of the subscriber certificate constitutes the subscriber's acceptance of the certificate. Failure of the subscriber to object to the certificate or its content, or the use of the certificate also constitutes certificate acceptance.

4.4.2 Publication of the certificate by the CA

Subscriber certificates issued by CAs within The Service will not be publicly available.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulations.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Use of the private key corresponding to the public key of the certificate will only be permitted once the subscriber has agreed to the subscriber terms and conditions of The Service, and accepted the certificate and its contents.
The certificate must only be used in accordance with the terms and conditions of The Service.

Subscriber certificates must only be used for their intended purpose, that is, be consistent with the KeyUsage field extensions included in the certificate.

Subscribers must protect their private keys and activation data from unauthorized use. Subscribers must discontinue the use of the private key following expiration or revocation of the certificate containing the associated public key, the only exception being using the private key for decryption of data earlier encrypted by the private key.

4.5.2 Relying party public key and certificate usage

Relying parties that use subscriber certificates issued within The Service to identify subscribers shall independently ensure:

- that certificates are only used to verify the identity of subscribers in accordance with this CP and CPS.
- that the certificates are being used in accordance with the KeyUsage field extensions included in the certificate.
- that the status of the certificate, and all the CAs in the chain that issued the certificate, are valid and not revoked.
- that the appropriate software or hardware is utilized to perform digital signature verification or other cryptographic operations in accordance with RFC5280, X.509 and applicable IETF PKIX standards. Such operations include verifying the validity of each certificate relied upon, identifying a certificate chain and verifying the digital signatures of all certificates in the certificate chain.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificate renewals are managed with the same procedure as new certificate applications.

4.7 Certificate re-key

Certificate re-keying is not allowed.

4.8 Certificate modification

Certificate modifications are managed with the same procedure as new certificate applications.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

The Service will revoke certificates issued within The Service under the following circumstances:

- If the unique identity, for example Subject serial number, and names of the subscriber whose information is contained in the Subject of the certificate are changed.
- If receiving a revocation request according to section 3.4.
- If the subscriber fails to retrieve the certificate within a reasonable time from the issuance of the certificate.
- If suspecting that a private key associated with a subscriber certificate has been compromised or used by some entity that is not the subscriber.
- If suspecting that the activation code for a private key associated with a subscriber certificate is known by an entity that is not the subscriber.
- If suspecting that the smart card, hardware token or equivalent cryptographic module, or mobile device that contains the private key is no longer in use, or possessed, by the subscriber.
- If suspecting that the subscriber violates the terms and conditions of The Service.
- If an error in production occurs within a processing center.
- If an RA organization terminates its relationship with The Service all certificates issued under the RA domain will be revoked.
- If PsPT detects or otherwise becomes aware that a court has revoked a Subscriber's right to use the Domain Name or Organizational information contained within subscriber certificates issued under an RA domain.
- If a CA key used within The Service is suspected to be compromised.
- If the use of a CA is terminated.
- In such additional events that PsPT determines, at its sole discretion, warrant revocation.

4.9.2 Who can request revocation

Revocation requests can be made by:

- the certificate subscriber
- a CA Officer, RA Officer, or other authorized applicant within the RA domain
- the applicable processing center
- the Service operational team

See section 3.4.

4.9.3 Procedure for revocation request

Entities submitting certificate revocation requests must be identified according to section 3.4.
RAs are required to promptly revoke certificates involved in a security incident.
The Service will:

- Revoke a certificate within a reasonable time if the request is authenticated in accordance with section 3.4.
- Provide a certificate management portal available 24 hours a day, all days of the year to allow RA Officers to make certificate revocation requests.
- Provide a self-service portal for subscribers to revoke their own certificates.
- Provide an OSCP service where information regarding certificate revocation status of issued certificates can be obtained throughout the validity of the issuing CA.
- List revoked certificates in applicable CRL. Expired certificates may be excluded from the CRLs.

For Processing centers, revocation requests may be systematically performed as long as the certificate being revoked is associated with the order being processed.

4.9.4 Revocation request grace period

Revocation requests must be submitted as promptly as possible.

4.9.5 Time within which CA must process the revocation request

The revocation request is processed within The Service promptly after receiving the revocation request.

4.9.6 Revocation checking requirement for relying parties

It is solely the responsibility of the relying parties to verify the validity and status of certificates issued in accordance with this CP and CPS before a certificate is used. Relying parties must verify revocation status through the OCSP service or CRLs identified in each certificate included in the certificate chain.

When conducting revocation control a relying party must make sure that:

- The certificate is within its validity time.
- The OCSP response is still valid.
- The digital signature of the OCSP response is valid.
- The revocation control is made against a current revocation list.
- The digital signature of the revocation list is valid.

4.9.7 CRL issuance frequency

The issuing CAs of The Service will normally update and issue new CRLs at least every 60 minutes. The NextUpdate field value of the CRL identifies the point in time when the CRL should be considered as expired and will be set to 48 hours.

The "Pointsharp SweID Root CA v1" is maintained in an off-line state and will issue a new CRL at least once per year or whenever a subordinate CA certificate is revoked. Root CA CRLs will have its NextUpdate attribute set to maximum one year after the issuance of the CRL.

Upon expiration of certain CAs, a final CRL MAY be published that has a NextUpdate value that exceeds the time parameters noted elsewhere in this section.

4.9.8 Maximum latency for CRLs

The publication of CRLs to the CRL repositories will normally be done without any delay but will not occur more than 60 minutes after CRL issuance.

4.9.9 Online revocation/status checking availability

The Service offers an OCSP service (Online revocation/status checking service) as the primary source of revocation information.
The OCSP service will be updated with the latest revocation status information from issuing CAs promptly after the revocation of a subscriber certificate.

Revocation status information in the OCSP services regarding issuing CA certificates will be updated with the latest revocation information every time a new CRL is issued by the Root CA.

4.9.10 Online revocation checking requirements

A relying party must confirm the revocation status of a certificate via the OCSP service or via the CRL in accordance with section 4.9.6, prior to relying on the certificate.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements related to key compromise

Entities participating in The Service are required to report certificate security incidents to PsPT.

In the event of the discovery or suspicion that a CA's private key has been compromised and therefore has been or is to be revoked all entities participating in The Service will be notified by Pointsharp. Pointsharp will also use reasonable efforts to notify potential relying parties other than RAs upon the revocation.

4.9.13 Circumstances for suspension

Certificate suspension is not allowed for certificates issued within The Service.

4.10 Certificate status services

4.10.1 Operational characteristics

The Service will make certificate status information available through an OCSP service according to section 4.9.9 and section 4.9.10. The Service will also make certificate status information available through the publishing of CRLs according to section 4.9.7 and section 4.9.8.

4.10.2 Service availability

The Service will provide certificate status information services 24 hours a day, all days of the year without interruption, excluding scheduled maintenance.

4.10.3 Optional features

No stipulations.

4.11 End of subscription

Subscribers may end their subscription to certificate services offered by The Service either by:

- requesting that their certificates be revoked, or
- allowing the certificates to expire.

4.12 Key escrow and recovery

Private keys will not be escrowed within The Service.

4.12.1 Key escrow and recovery policy practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical security controls

5.1.1 Site location and construction

CA systems, other systems, and server applications necessary to maintain The Service are operated within secure PCI-DSS approved data centers located in Sweden. Physical and logical access controls are implemented to make the operations inaccessible to non-authorized personnel.
The site locations and constructions, when combined with other physical security

protection mechanisms such as guards, door locks, and intrusion sensors, provide robust protection against unauthorized access to the CA systems, services, documentation, and records.
The data centers employ active surveillance and alarms monitored by guards 24 hours a day, all days of the year.

Multiple data centers are used to ensure "High-Availability" for The Service operations, and measures have been taken in each data center to an extent that is considered sufficient to maintain High-Availability locally.
The same as applies above for data centers also applies for processing centers used within The Service for manufacturing and personalization of smart cards.

The central administration of CA server applications and other applications necessary for The Service is located in the Pointsharp premises. HSM operations, see section 5.2.1 and the "HSM Officer" Trusted role, are handled from the same location. Physical and logical access controls are implemented to make the premises inaccessible to non-authorized personnel. The premises employ active surveillance with intrusion alarms, sensors, and cameras monitored by a security company 24 hours all days of the year. Administration of applications and specific HSM operations are handled in a separate locked room within the premises and network segmentation is used for logical protection. Only authorized personnel with Trusted roles have access to the room. When not used all sensitive information and materials are stored in safes or locked containers.

All RA Officer tasks performed within RA domains must be carried out at premises with physical and logical access controls. All RA tasks are done in web based applications provided by The Service and no subscriber data related to The Service is stored at the RA premises.

The RA organization's compliance to physical security controls, according to The RA Trust Framework and this CP and CPS, must be described in the RA Declaration of Compliance made before being allowed to take part as an RA within The Service.

5.1.2 Physical access

For security reasons, detailed information on security procedures for physical access to data centers, processing centers, and Pointsharp's premises is not publicly available. Detailed information regarding physical access is described in the operational documentation of The Service.

All system components (computers, services, applications, documentation, records, rooms, etc.) and supporting services (UPS, power, cooling, etc.) are protected from unauthorized access and physical controls are implemented to reduce the risk of components being tampered with.
The data centers and processing centers are monitored by guards 24 hours a day, all days of the year. Intrusion alarms, cameras, and detectors are monitored by the guards.
All access is monitored and logged.

Pointsharp's premises have intrusion alarms, cameras, and detectors, and are monitored by a security company 24 hours a day, all days of the year. Administration of applications used in The Service and management of HSMs, see section 5.2.1 and

the "HSM Officer" Trusted role, are handled from a separate locked room with physical access controls.

Unescorted access to the data centers, processing centers, and Pointsharp premises is limited to authorized personnel identified on access lists. Personnel that is not included on the access lists must be escorted by authorized personnel and supervised during their work. Visitors to data centers and processing centers will be registered in a visitors log.

Physical controls are in place to ensure that at least two persons in Trusted roles are needed to get physical access to HSMs, HSM backups, and other physical equipment related to the use and management of CA private keys.
The only exception being that one-person access is allowed to the server racks with online HSMs but such access is monitored by CCTV.
Online HSM's cannot be removed or managed locally without at least three persons in Trusted Roles being present.

All removable media and paper documentation containing sensitive information related to operations of The Service are stored in safes. Physical security mechanisms are implemented at an appropriate level and are dependent on the level of threat to the equipment or information needing protection, and the sensitivity of the information.

Physical access requirements for RA organizations are described and agreed upon in the Customer Agreement and The RA Trust Framework. Tasks must be carried out in controlled office environments where access is restricted to authorized personnel. No keys (smart cards and hardware tokens) or codes may be left unmonitored.

5.1.3 Power and air conditioning

Backup power systems and environmental controls are used to protect the CA systems and other systems necessary to maintain The Service.

The rooms in the data center with UPS systems are protected at the same level as the server rooms regarding climate (cooling), alarms, and fire extinguishers. UPSs are divided into two separate systems for redundancy. Each system is designed with modules that give additional redundancy. The UPSs are periodically tested, multiple times per year, with load.

From the UPS rooms, power is distributed in the server rooms with local distribution centers for A and B power. In each server rack, there are separate PDUs mounted for the A and B power.
Service outlets are available in the production hall.

Backup power is available in the form of three diesel generators for redundancy.
Fuel is available on-site for more than 3 days of operation at full load.
In the backup power room, there are fire alarms, technical alarms, and fixed installations of fire extinguishing.

The cooling in each hall is provided by circulating units connected to brine systems. Redundancy is available both on the media side and on the unit side.

5.1.4 Water exposure

Pointsharp has taken reasonable precautions to minimize the impact of water exposure to systems used by The Service.

In the data center, there are liquids in the halls in the form of refrigerants for the circulation units. There is also condensate drainage where condensation water from circulation units is conducted to floor wells in the halls. The floor wells are equipped with a non-return valve and open into a pump pit without a fixed connection to the drainage trunk.
Water alarms are available, for instance, detecting the presence of water on the floors.

5.1.5 Fire prevention and protection

Pointsharp has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke.

Fire alarms in the data center are in the form of an aspirational alarm. The alarm is connected to SOS and emergency services. Fixed extinguishing system is installed using INERGEN gas. Handheld fire extinguishers are also available with CO_2 as extinguishing media.

The Pointsharp premises has water sprinkling systems and handheld fire extinguishers.

5.1.6 Media storage

All media containing production software and data, audit, archive, or backup information is stored within the data center, Pointsharp's premises, processing center, or in secure off-site storage premises with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

A number of safes are used off-site from the data center to store and protect key backups, key material, confidential documentation, and other documentation important for The Service. Some safes are equipped with individually lockable security cabinets that are used by Pointsharp personnel for storing tokens and other information related to their role. All access to the contents in safes and safe cabinets requires at least two persons in duality and all access are logged electronically or manually. This is to provide protection against theft, corruption, destruction, or unauthorized use of the stored information.

5.1.7 Waste disposal

Information or materials that are sensitive must be shredded or destroyed before disposal.

Electronic waste is permanently wiped and software for permanently destroying data is used. Cryptographic devices are physically destroyed or erased in accordance with the manufacturers' guidance prior to disposal.
Duality is required when destroying the most sensitive documentation, data, and hardware, and such destruction is logged.

Other waste is disposed of in accordance with normal waste disposal requirements.

5.1.8 Off-site backup

The Service continuously performs backups of data and backups of critical data are made at least on an hourly basis. Backups are kept in encrypted form and are automatically and securely transferred to and stored in at least one off-site location. The off-site locations have procedural and physical controls implemented that corresponds to the backups' operational location.

5.2 Procedural controls

5.2.1 Trusted roles

Trusted roles include all Pointsharp employees and consultants, personnel at subcontractors, and RA personnel that have access to or control authentication, cryptographic operations, and information that may materially affect:

- administration related to CA private keys
- management and configuration of critical systems and applications used by The Service
- validation of information in certificate applications and/or approving or rejecting applications
- managing revocation requests
- integrity of the repository and archives

Pointsharp AB, PsPT, or authorized representatives of subcontractors, and RAs are responsible for appointing individuals to Trusted roles.

Trusted roles includes at least, but are not limited to, the roles described in the following tables.

1 Trusted roles at CA (Pointsharp)

Trusted role	Responsibilities
Security Manager	Overall responsible for the security work within the operations and management of The Service. This includes information security and GDPR as well as physical security. The Security Manager is not directly involved in the processes of generating certificates, smart cards, or revocation lists but is responsible for that all operative roles act within the boundaries of its permissions.
Local Security Officer	Responsible at the data centers and processing centers for the local compliance to this CP and CPS, and other agreements concerning the operations of The Service.

Trusted role	Responsibilities
System Administrator	Technical operational personnel at the data center. Acting as administrator of system resources. Typical tasks include: • maintaining systems, application operations, and arranging repairs in the event of system incidents • maintaining system software integrity • installing software updates and patches • handling system backups and tests restoring of backup data • verifying that peripherals are working properly • monitoring system performance
CA Administrator	Acts as administrator of the CA system applications. Typical tasks include: • managing access to CA system applications • configuration of and changes in CA's use of CA keys • issuing and revocation of CA certificates • issuing and revocation of OCSP and RA system certificates • creation and changes of certificate profiles • CA instance configuration • RA instance configuration • CRL and OCSP configurations
Database Manager	Operational role managing the databases used within The Service including securing proper encryption of sensitive data handled in the databases.
HSM System Administrator	Technical operational personnel acting as administrator for the application used for administration of the HSM appliance. Performing tasks within the HSM supervised by HSM Officers. Manages CA keys under the supervision of two or more HSM Officers.
HSM Officer	General name for a number of HSM Officer roles, assigned to different individuals to maintain separation of duties, with the responsibilities for the following tasks: • top admin for HSMs. Allows for policy changes as creation of other roles. Creates, configures, and deletes partitions • admin for a logical container of an HSM partition. Also manages HSM partitions to be cloned and to participate in HA implementations • management and use of objects in an HSM partition. Connects as a client to HSM partitions • enabling of network connections to give remote PEDs access to HSMs • auditing of all actions that have taken place in HSMs

Trusted role	Responsibilities
HSM Safe Manager	Individual holding keys, tokens or passwords necessary to open safes with HSMs, HSM backups or other sensitive materials related to the management of HSMs and CA private keys. A minimum of two HSM Safe Managers are needed to open such safes.
PoSC Administrator	Operational role in the subscriber and certificate management application. Typical tasks include: • configuring subscriber smart card and certificate templates • configuring of certificate application and issuing processes • configuring of user groups and privileges for user groups • managing access for other personnel in Trusted roles within the application • adding, changing, and deleting customer (RA) configurations
CA Officer	Operational role in the subscriber and certificate management application for central RA functions performed within The Service (Service RA). Typical tasks include: Related to RA domains: • managing of first subscribers within a new RA domain • making applications of certificates and smart cards for the first RA personnel at a new RA domain • assisting RA domains with subscriber and subscriber certificate management (certificate application, certificate issuing, and certificate revocation) when necessary • conducting identity verification upon certificate application and extradition Related to The Service and Pointsharp operations: • managing of subscribers • making subscriber certificate applications • approving subscriber certificate applications • revoking subscriber certificates, smart cards, and tokens • conducting identity verification upon certificate application and extradition
Internal Auditor	External part appointed by Pointsharp. • performing compliance audits to determine whether Pointsharp is operating The Service in accordance with this CP and CPS, The RA Trust Framework, and other regulations that may apply.

Trusted role	Responsibilities
Local Auditor	An administrative role. Typical tasks include: • reviewing, maintaining, and archiving audit logs • checking integrity of audit logs • having read access to application audit logs but cannot change, modify, or delete any log entries • performing internal audits to determine whether personnel involved in operations of The Service are operating in accordance with this CP and CPS, The RA Trust Framework, and other regulations that may apply. • performing compliance audits on subcontractors and RAs to determine whether other organizations involved in operations of The Service are operating in accordance with this CP and CPS, The RA Trust Framework, subcontractor agreements, and other regulations and agreements that may apply.

2 Trusted roles at RAs

Trusted role at RA	Responsibilities
RA Security Officer	Administrative role responsible for the compliance work at a specific RA domain. Typical tasks include: • controlling and evaluating compliance to the RA's obligations according to the Customer Agreement, The RA Trust Framework, and this CP and CPS • reporting incidents and deviations to Pointsharp • evaluating personnel before being appointed to a trusted role at the RA.
RA Auditor	Operational role responsible for internal auditing of the RA organization. Typical tasks include: • evaluating the RA organization's compliance with processes for the management of subscribers and e-identities. • performing internal audits regarding the management of e-identities. • supervising the RA Officers.
RA Officer	Operational role in the subscriber and certificate management application for a specific RA domain. Typical tasks include: • managing of subscribers • managing access configurations for other personnel in Trusted roles within the RA domain. • making subscriber certificate applications • conducting identity verification upon certificate application and extradition • approving subscriber certificate applications • issuing subscriber certificates • revoking subscriber certificates, smart cards, and tokens • assigning subscriber roles within the RA domain.

Pointsharp has chosen to divide most of the Trusted roles mentioned in the tables above further into different sub roles. All Trusted roles are documented in the operational documentation of The Service and is not publicly available.

5.2.2 Number of persons required per task

Sensitive tasks require the collaboration of multiple persons in Trusted roles. At least the following tasks will only be allowed to be performed with multi-person control ("n" out of "m"), where "n" needs to be at least 2 persons.

- Administration of HSMs and CA keys
- Access safes with CA keys and backups of CA keys
- Locks securing online HSMs in server racks and preventing access to control buttons and ports
- Access to safes with personal crypto keys for HSM administration
- Configuration of sensitive applications, for example, CMS, OCSP, subscriber and certificate management application
- Issuing of CA and OCSP certificates
- Issuing of Subscriber certificates
- Access to data in databases (data and audit logs)
- Access to audit logs in CA system and HSMs.
- Access to archives.

Multi-person control may be enforced electronically, physically, or by manual procedures, or combinations of the controls mentioned.

For tasks only requiring one person in a Trusted role the authentication requirements are as mentioned in section 5.2.3. All user initiated actions in systems and applications are logged in a way that they can be linked to an individual user, and will be subject to reviews.

- Access to application servers
- Access to database servers
- Access to backups
- Access to application trace files

Physical access to server racks with online HSMs is monitored by CCTV cameras to ensure that HSMs are not tampered with.

5.2.3 Identification and authentication for each role

Smart cards with LoA4 or LoA3 certificates will be used by personnel with Trusted roles for authentication when accessing systems and applications that are part of The Service.
Where not possible to use certificates for authentication other MFA methods will be used.

Before obtaining a smart card, hardware token or other MFA token all individuals are required to have an in-person meeting with a CA Officer, an RA Officer or other representative acting on behalf of the CA and are obliged to present an approved Swedish identification document proving their identity.

Personnel issuing and administrating certificates, except for RA Officers only involved in the issuing of LoA3 certificates, will use LoA4 certificates issued by The Service for authentication.
RA Officers only being involved in the issuing and administration of LoA3 certificates will at least use LoA3 certificates issued by The Service, or by another issuer complying with the Swedish eID Assurance Framework and being approved by PsPT, for authentication.

Central systems involved in the operations of The Service may allow access with a lower grade of authentication but only if ("n" out of "m") multi-person control is applied.

5.2.4 Roles requiring separation of duties

Pointsharp maintains and enforces a policy to ensure separation of duties for critical CA and RA functions to prevent one individual from maliciously using or compromising The Service without detection.
The complete documentation of roles, and which roles can be held by the same individual are found in the operational documentation of The Service and is not publicly available.
Separation of duties may be enforced electronically or by manual procedures.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Trusted roles will be assigned to employees presenting proof of trustworthiness, proper qualifications, and education. The same controls apply whether the Trusted role is appointed to a Pointsharp employee, consultant, personnel at a subcontractor, or RA personnel.

All personnel in Trusted roles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations. Trusted roles will not be approved for personnel having other conflicting roles.

5.3.2 Background check procedures

Background checks are done for all personnel given a Trusted role at the CA and for all other personnel when employed by Pointsharp. The demand for background checks applies whether a Trusted role is appointed to a Pointsharp employee, a consultant, personnel of a subcontractor, or personnel at an RA organization.
Background checks include but are not limited to

- identity control at a physical meeting,
- control of current and previous employments,
- suitability assessment for the position,
- completed relevant training,
- controls of financial status, and
- review of criminal records.

Parts of the background checks for personnel in Trusted roles at the CA are reviewed periodically and failing a review will result in the person being removed from the Trusted role.

All RA organizations must set up its own process for background checks of RA personnel.

5.3.3 Training requirements

Pointsharp conducts training and retraining for all its personnel involved in The Service, to the extent required to ensure that such personnel maintains the necessary skills to perform their job responsibilities in a competent and satisfactory manner. Documented training of personnel is required before taking on a Trusted role. Subcontractors and RAs are also required to carry out training for personnel in Trusted roles before allowing them to enter such roles.

There relevant for the role, personnel will for instance get training in deeper PKI understanding, application management, certificate issuance processes, ITIL processes, disaster recovery routines, thorough security framework training, and security processes including handling safes and CA private keys.

Training will always include basic PKI concepts, relevant parts concerning information security, incident reporting, and procedures to handle and protect of subscribers' personal data.

5.3.4 Retraining frequency and requirements

Retraining of Pointsharp personnel will be carried out at least every 12 months or whenever significant changes are made to The Service or part of The Service.

Subcontractors and RAs are also required to carry out retraining for personnel in Trusted roles at least every 12 months.

5.3.5 Job rotation frequency and sequence

No stipulations

5.3.6 Sanctions for unauthorized actions

Pointsharp, subcontractors, and RAs must ensure that appropriate action is taken against personnel who violates this CP and CPS. Depending on the severity, further actions could be taken by warnings, relief from the Trusted role or other roles within The Service, or termination of employment. In the event of a crime related to the violation, a report will be made to the police.

5.3.7 Independent contractor requirements

Only Pointsharp employees will have Trusted roles related to the management of HSMs and CA private keys. Other Trusted roles within The Service may be given to consultants or personnel at subcontractors, or RA personnel.
All roles, including other than Trusted roles, will require to fulfill the background checks according to section 5.3.2, before assigning a role to an individual.

5.3.8 Documentation supplied to personnel

The Service will provide relevant documentation and tools necessary for all personnel involved in The Service to perform their duties. The documentation and tools are including, but are not limited to the following:

- This CP and CPS and other specific policies
- Applications' operational guides
- System documentation
- Procedures
- Educational material

5.4 Audit logging procedures

5.4.1 Types of events recorded

At least the following events related to operations of The Service are manually or automatically recorded within logs:

Security-related events:

- Creation of and changes in user account and access permissions
- Failed logon attempts
- Successful logon
- Software installation and configuration
- Changes in security-sensitive files or records
- PKI and security system actions made by personnel at Pointsharp or subcontractors
- System reboot
- System or application failure
- Firewall configurations
- Network activity
- Intrusion detection
- Malware detection

CA life cycle management events:

- CA key generation, backup, storage, recovery, archival, and destruction
- HSM device life cycle management events
- CA certificate issuance
- OCSP certificate issuance
- CA and OCSP certificate revocation
- CRL generation and issuance
- Successful or unsuccessful processing of requests

Physical access to:

- Data centers, processing center, and CA management premises
- Safes with sensitive data like HSMs with CA private keys
- Archives

Subscriber certificate events initiated at RA, CA, or processing center:

- Subscriber management

- Certificate applications including information of identity document presented by the Subscriber
- Certificate issuing requests including the identity of the requestor
- Successful or unsuccessful processing of requests
- Certificate revocation

Log entries include the following:

- Date and time
- Serial or sequence number of the log entry
- Identity of the entity making the entry
- Entry type

5.4.2 Frequency of processing log

Pointsharp will at least every month review audit logs related to the certificate and Subscriber management and central security controls. Logs related to CA systems, encryption of databases, and online HSMs will undergo quarterly audit reviews. Other logs, for example, Offline HSM and physical access logs to safes, will be reviewed with other periodicities but at least every 12 months.

The data center and processing center providers are ISO/IEC 27001 compliant and have processes and routines to perform regular checks of event logs.

System and file integrity checks are done on regular basis. Some security and integrity-related events are automatically sent for automated review to check for warnings and abnormal activities.

5.4.3 Retention period for audit log

Pointsharp will retain audit logs, according to section 5.4.1, for at least five (5) years after the last Subscriber certificate has expired. Audit logs are kept on-site at least until they have been reviewed and are collected periodically for archival.

5.4.4 Protection of audit log

Audit logs are protected from unauthorized viewing and any kind of modification, deletion, or other tampering. This is secured by encryption and physical and electronic security controls. Only personnel in Trusted roles have access to audit logs.

Procedures are implemented that protect archived data from destruction prior to the end of the audit log retention period.

The Service may disclose audit logs to relevant parties, for example, Auditors and authorized RA representatives, upon request and if not prohibited by applicable law.

5.4.5 Audit log backup procedures

Incremental backups of audit logs are created hourly and full backups are performed at least weekly. Backup copies will be stored off-site.

5.4.6 Audit collection system (internal vs. external)

Applications built-in audit mechanisms are used and controlled manually.
An internal automated audit collection system is used for configurations, network and operating system-level events, and some specific application events.

All manual controls are made by personnel in Trusted roles.

5.4.7 Notification to event-causing subject

No stipulations.

5.4.8 Vulnerability assessments

Pointsharp will perform risk analysis and vulnerability assessments of The Service when needed but at least annually. Based on the assessment results, policies, operations and practices are revised, if necessary.

Vulnerability checks and penetration tests will be performed on critical systems in connection with major upgrades and at least annually.

5.5 Records archival

5.5.1 Types of records archived

All logs according to section 5.4.1 are archived as well as other database records and all information provided in the repository according to section 2.1, whether publicly available or not. However, revocation status will be archived within the database and log records, not as individual CRLs and OCSP responses.
All subcontractor and Customer Agreements are archived.

5.5.2 Retention period for archive

Pointsharp will retain archived data for at least five (5) years from the time of data generation unless a greater retention period is required by any other applicable law or local policy.

5.5.3 Protection of archive

The Service will store its archived records at a secure off-site location, other than the data center, in a manner that prevents unauthorized access, modification, substitution, or destruction. At least two persons in Trusted roles are needed to access sensitive archived data both electronically and physically at the off-site location.
Sensitive records are digitally signed and encrypted.

5.5.4 Archive backup procedures

Information to be archived is collected from the places of origin at defined intervals and transferred to the archives.

Pointsharp will backup electronic archives on a periodical basis and when necessary. Backups and copies of physical archives will be stored in separate secure locations separated from the location of the archives.

5.5.5 Requirements for time-stamping of records

The Network Time Protocol (NTP) is used to synchronize clocks in all systems used for the creation of records like audit logs, signatures, database records, and other information there it is essential to use correct time. Three different NTP servers are used and are in their turn synchronized with an external UTC time source.

All documentation archived pursuant to this section will be marked with the date of their creation or execution.

5.5.6 Archive collection system (internal or external)

The Service will collect and archive information internally within Pointsharp.

5.5.7 Procedures to obtain and verify archive information

The Service will not release archives unless requested by PsPT or as required by law. Only personnel in Trusted roles with authorization are able to obtain access to the archives. The integrity of information is verified when it is restored from the archive.

The Service may allow subscribers and accountable issuers to obtain a copy of their own archived Information.

5.6 Key changeover

A CA certificate may be renewed upon approval from the PsPT.
New CA key pairs will be generated according to section 6.1 and the old key pairs will be retired according to section 6.3.2. A new CA certificate containing the new CA public key will be issued and published on the repository.

After the key changeover, The Service will only use the new key to sign certificates. The old CA private key will still be protected in the same manner as before the key changeover. The Service will continue to use the private key to sign revocation checking information and the old CA certificate will remain available to verify signatures until all of the certificates signed with the old private key have expired.

The key changeover will take place at least 3 months prior to the expiration time for an existing CA certificate.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Change and incident management processes are implemented to allow for proper handling of incidents and recovery of any disasters that may occur.

All components used for the operations of The Service, including server applications, CA server, HSMs, and OCSP responders, are located in at least two different data center locations to ensure high availability. Backup data is sent to a third off-site location. Backups of all data critical to The Service are made on at least an hourly basis and are periodically tested.

A business continuity plan and a disaster recovery plan are in effect to maintain robust and secure operations. The disaster recovery plan is tested at least every sixth month.

Priority will be given to re-establishing the generation of certificate status information (OCSP service and CRLs) and thereafter certificate revocation and issuance.

5.7.2 Computing resources, software, and/or data are corrupted

In the event of the corruption of computing resources, software, and/or data, the incident management procedures are initiated.

The Service will be able to restore from corrupted software and data using the last known correct backups. Audit logs will be reviewed to ensure corrections of any missing data from the period between the used backup and the time of corruption.

In case of hardware corruption and after ensuring the integrity of the CA systems, The Service will re-initiate its operations on replacement hardware located at a secure facility, using backup copies of its software, data, and CA private keys.

If necessary, disaster recovery procedures will be initiated.

Pointsharp stores backup copies of its CA private keys in secure off-site locations and backups of other critical data are done on at least an hourly basis.

5.7.3 Entity private key compromise procedures

If Pointsharp suspects that a CA private key has been comprised or lost then Pointsharp will follow the incident process for high priority incidents and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action.

In such an event, that the incident assessment shows it is necessary to revoke the CA, Pointsharp will take the following steps:

- The CA certificate and the related private key will be revoked. The CRL of the Root CA will be updated with revocation information of the revoked CA and published.
- Remove all forms of certificate checking services for certificates issued by the compromised CA. This means removing and ceasing with all publications of revocation lists issued by the compromised CA and ceasing OCSP services for the compromised CA. When revocation information is unavailable, the relying parties must consider all certificates issued by the compromised CA as revoked.
- Inform all parties with which The Service has a relationship, and publish information in the repository, that the CA's private key has been compromised and how The Service will be recovered.

After a CA private key compromise Pointsharp personnel must report the results of the investigation. The report must detail the cause of the compromise or loss and the measures that should be taken to prevent a reoccurrence.

Following the revocation of a CA within The Service, Pointsharp will generate a new CA Key Pair and sign a new CA certificate in accordance with this CP and CPS. The new CA certificate will be distributed in accordance with section 6.1.4.

5.7.4 Business continuity capabilities after a disaster

The Service will provide business continuity procedures in a Disaster recovery plan that outlines the steps to be taken in the event of corruption or loss of computing resources, software, and/or data. The Disaster recovery plan also contains instructions for periodic verification of procedures and material needed.

All components in the data center are mirrored in a secondary location in order to maintain business continuity capabilities.
Pointsharp will continuously verify backup and restore procedures to be prepared for the event that all sites suffer a disaster simultaneously. Backup and restore procedures will be tested at least every sixth months.

5.8 CA or RA termination

If an RA (customer) is terminated from The Service, the customer must uninstall relevant software provided by Pointsharp and all certificates issued within the RA domain will be revoked.
This might for instance be the case if a Customer Agreement is terminated by an RA, if an RA do not fulfill the obligations according to the Customer Agreement or if an RA does not comply with The RA Trust Framework or the provisions in this CP and CPS.

In the event that a CA within The Service is planned to be terminated, Pointsharp will make a commercially reasonable effort to inform customers, relying parties and other affected parties at least one (1) year in advance. Upon CA termination, at least the following steps will be taken:

- All certificates that have been issued by the CA and still are valid will be revoked.
- The Service will cease publishing revocation checking information, that is, the OCSP service and CRLs related to the CA will be removed.
- All permissions for RAs related to the CA will be terminated.
- All archives and logs will be kept for the stated archival period.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Pointsharp will generate and protect cryptographic keying material for CAs on cryptographic hardware security modules "HSMs" using multiple individuals acting in Trusted roles. When generating keying material, Pointsharp creates auditable evidence to show that The Service enforced role separation and followed its key generation process.

The method used for generation of subscriber key pairs depends on how the private keys are protected and the CA used for issuing of the subscriber certificates associated with the keys, as described in the table below.

Issuing CA	Key protection	Key generation
Pointsharp SweID 4 CA vX	Smart card	Key pairs are generated at the processing center used by The Service and stored on the smart card. Key pairs are generated in one of two ways: • internally on the smart card (onboard key generation). • in an HSM and then securely transferred to the smart card. HSMs may be used for key pair generation for performance reasons.
Pointsharp SweID 3 CA vX	Smart card, primary	Key pairs are generated at the processing center used by The Service and stored on the smart card. Key pairs are generated in one of two ways: • internally on the smart card (onboard key generation). • in an HSM and then securely transferred to the smart card. HSMs may be used for key pair generation for performance reasons.
	Smart card, temporary	Key pairs are generated on the smart card at the premises of Pointsharp or at the premises of the RA.
	Smart card, derived	Key pairs are generated on the smart card by the subscriber. The smart card has been issued by The Service or by another issuer approved by The Service and being compliant to the Swedish eID Assurance Framework.
	Hardware token	Key pairs are generated on the Hardware token at the premises of Pointsharp or at the premises of the RA.
Pointsharp SweID Mobile 3 CA vX	Mobile app	Key pairs are generated within a secure mobile app delivered by Pointsharp and are stored in a PIN-protected soft token within the app. The secure app uses random number generation according to NIST SP800-90A.

6.1.2 Private key delivery to subscriber

Depending on generating and delivery method of private keys, delivery method for activation data and the quality of the subscriber identification, different identity assurance levels are achieved.

Private key delivery to subscribers must always be preceded by an identification of the subscriber.

The method used for private key delivery to the subscriber depends on how the private keys are protected and the CA used for issuing of the subscriber certificates associated with the private key:

Issuing CA	Key protection	Key delivery
Pointsharp SweID 4 CA vX	Smart card	Smart cards are delivered from the processing center to the office of the RA or CA that made the certificate application on behalf of the subscriber. PIN/PUK related to the private keys stored on the smart card are sent to the subscriber's home address according to the SPAR service.The subscriber receives the smart card with the private keys from an RA or CA Officer after having presented a valid identification document, and having accepted the terms and conditions for the use of the subscriber certificates. The subscriber acknowledges receiving the smart card (private keys) and acceptance of the terms and conditions with a digital signature using the signature PIN related to the signature private key on the smart card.
Pointsharp SweID 3 CA vX	Smart card, primary	Smart cards are delivered from the processing center to the office of the RA or CA that made the certificate application on behalf of the subscriber. The subscriber receives the smart card with the private keys from an RA or CA Officer after having presented a valid identity document and having accepted the subscriber terms and conditions for the use of the subscriber certificates. PINs associated with the private keys are set by the subscriber. The subscriber acknowledges receiving the smart card (private keys) and acceptance of the terms and conditions with a digital signature using the signature PIN related to the signature private key on the smart card.
	Smart card, temporary	Smart cards are personalized at the premises of the RA or the premises of Pointsharp with the subscriber present. Before the issuing process, the subscriber is identified by presenting a valid identity document to the RA Officer or the CA Officer. After the key generation and certificate issuance, PINs associated with the private keys are set by the subscriber. The subscriber acknowledges receiving the smart card (private keys) and acceptance of the subscriber terms and conditions with a digital signature using the signature PIN related to the signature private key on the smart card and receives the smart card.

Issuing CA	Key protection	Key delivery
	Smart card, derived	The subscriber uses a trusted authentication certificate of at least LoA3, issued by The Service or another issuer approved by The Service and being compliant to the Swedish eID Assurance Framework, to authenticate with a self-service portal provided by The Service. The private key related to the trusted certificate must be protected on a smart card. After the subscriber has approved acceptance of the subscriber terms and conditions with a digital signature using the trusted authentication certificate, the enrolment of the derived certificate is started. The private keys and the associated PINs will be generated in one of two ways: • the private keys are generated on the smart card associated with the trusted certificate and the current PINs of the smart card are used. • the private keys are generated on a new smart card available to the subscriber and the PINs associated with the private keys are set by the subscriber after the issuance of the derived certificate.
	Hardware token	Hardware tokens are personalized at the premises of the RA or the premises of Pointsharp with the subscriber present. Before the issuing process, the subscriber is identified by presenting a valid identity document to the RA Officer or the CA Officer. After the key generation and certificate issuance, the PIN associated with the private key is set by the subscriber. The subscriber acknowledges receiving the Hardware token (private key) and acceptance of the subscriber terms and conditions with a digital signature using either the signature PIN related to the signature private key or the authentication PIN related to the authentication private key on the hardware token (no signature key pair is generated for some hardware tokens due to lack of functionality) and receives the token.

Issuing CA	Key protection	Key delivery
Pointsharp SweID Mobile 3 CA vX	Mobile app, in person	The subscriber certificate is enroled to the mobile app at the premises of the RA or the premises of Pointsharp with the subscriber present. Before the issuing process, the subscriber is identified by presenting a valid identity document to the RA Officer or the CA Officer. An activation code is presented to the subscriber and the subscriber is informed that by using the activation code the subscriber will acknowledge receiving the software token (private key) and the acceptance of the subscriber terms and conditions. The subscriber then uses the activation code in the mobile app and the issuing process is continued. Private keys are generated within the mobile app and are finally stored in a PIN-protected soft token within the app.
	Mobile app, derived	The subscriber uses a trusted authentication certificate of at least LoA3, issued by The Service or another issuer approved by The Service and being compliant to the Swedish eID Assurance Framework, to authenticate with a self-service portal provided by The Service. After the subscriber has approved acceptance of the subscriber terms and conditions with a digital signature using the trusted certificate, an activation code is presented to the subscriber. By using the activation code in the mobile, the issuing process is continued and private keys are generated within the mobile app and are finally stored in a PIN-protected soft token within the app.

6.1.3 Public key delivery to certificate issuer

Public keys must be delivered to The Service in a secure fashion and in a manner which binds the Subscriber's verified identity to the public key.
This is accomplished by including the public key in the certificate requests initiated by RA Officers, CA Officers, processing centers, and the subscribers.

Public key delivery to subscribers must always be preceded by an identification of the subscriber during the application process leading up to the certificate request.

6.1.4 CA public key delivery to relying parties

CA certificates with the CAs public keys are publicly available to relying parties and customers via the repository of The Service: https://repository.pointsharpsecurecloud.com.

6.1.5 Key sizes

The Service will follow the NIST recommendations, according to the latest version of "NIST Special Publication 800-57 Part 1" regarding the use of key sizes and hash algorithms.

- CA keys must be RSA keys with a length of at least 4096 bits and the hash algorithm used must be at least SHA-256.
- Subscriber keys, and keys used for the signature of CRLs and OCSP responses, must be RSA keys with a length of at least 2048 bits and the hash algorithm used must be at least SHA-256.

Any subcriber private keys with associated certificates expiring after 2030-12-31 must use RSA-keys with a length of at least 3072 bits.

6.1.6 Public key parameters generation and quality checking

The Service will generate public key parameters for CAs and perform parameter quality checking in accordance with NIST FIPS 140-2 level 3.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Certificates issued by The Service will include key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in X.509 v3 compliant software.

Key usages and extended key usages used in the certificates are specified in the certificate profiles. The certificate profiles are found in the Certificate and CRL specifications that are available at the online repository in accordance with section 2.1.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The procedures dictated by this CP regarding generation, storage and distribution of private keys are intended to provide protection for private keys in a way that minimizes the risk for keys to be inappropriately or maliciously exposed or used.

All CA cryptographic operations within The Service must be processed within HSMs rated to minimum FIPS 140-2 level 3 or Common Criteria EAL4+.

Subscribers' private keys must be stored, used and protected in a fashion that prevents key compromise and unauthorized access.

Subscribers' private keys will be protected in one of the following ways depending on issuing CA:

- CAs: "Pointsharp SweID 4 CA vX" and "Pointsharp SweID 3 CA vX":
  Subscriber keys are generated, stored, and protected in the smart card or the hardware token. For processes there smart cards and subscriber keys are generated in a processing center the use of HSMs are allowed for subscriber key generation. After generation the private and public keys are securely transferred to the smart card. Cryptographic modules used (HSMs, smart cards, and

hardware tokens) must be rated to minimum FIPS 140-2 level 3 or Common Criteria EAL4+.
- CA: "Pointsharp SweID Mobile 3 CA vX":
  Subscriber keys are generated and stored in a soft token within a secure mobile app provided by The Service. Due to security reasons, more information regarding the key generation and the key protection in the mobile app is not publicly available.

Subscribers are committed to comply with terms and conditions of The Service and thereby bound to protect the private keys in accordance with section 9.6.3.

6.2.2 Private key ("n" from "m") multi-person control

The Service has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations.
The Service operations uses "secret sharing" to split the activation and recovery data needed to make use of a CA private key into separate parts called "secret shares" held by individuals called shareholders. A threshold number of Secret Shares (n) out of the total number of Secret Shares (m) created and distributed for a particular HSM is required to activate or recover a CA private key stored on the HSM.
At least two persons are required for all processes involving HSMs. In most cases three or more persons need to be involved in a process due to separation of duties.

Smart cards with LoA4 certificates issued by The Service are required for all operational CA roles used for the management of the CAs.

6.2.3 Private key escrow

Key escrow is not allowed for any private keys generated or used within The Service.

6.2.4 Private key backup

Backups are made of CAs' private keys to secure the availability of The Service. The key backups are secured in Backup HSMs that are stored securely under security procedures equivalent with the security procedures used for the online HSMs used within The Service operations.

Multi-person controls and separation of duties mechanisms are used for the recovery process of private CA keys from Backup HSMs in the event of an incident, see section 6.2.2.

6.2.5 Private key archival

No archival will be done of any CA or subscriber private keys generated within The Service.

6.2.6 Private key transfer into or from a cryptographic module

All CA private keys are generated within an HSM. CA private keys will be backed up to separate HSMs, intended specifically for backups (Backup HSMs), via secure indirect communication between the HSMs.

6.2.7 Private key storage on cryptographic module

CA private keys are generated and stored within an HSM, see section 6.2.1.

For information regarding subscribers' private keys, see section 6.2.1.

6.2.8 Method of activating private key

At least two persons in Trusted roles are required for the activation of the CA private keys. The individuals are authenticated either by a two-factor method provided by the HSM manufacturer or by a LoA4 certificate issued by The Service, depending on the action.

All information exchange between an RA and the CA is encrypted. All CA and RA personnel are authenticated in the systems of The Service in accordance with section 5.2.3 and actions resulting in the use of a CAs' private issuer keys are authenticated by the system based on a digital signature.

The method used for activation of subscribers' private keys depends on how the private keys are protected and the CA used for issuing of the subscriber certificates associated with the keys, see the following table.

Issuing CA	Key protection	Method of activation
Pointsharp SweiD 4 CA vX	Smart card	PIN/PUK related to the private keys stored on the smart card are sent to the subscribers home address according to the SPAR service.The subscriber uses the PIN related to a private key to activate it.
Pointsharp SweID 3 CA vX	Smart card, primary	The PUK of the smart card is received from the processing center and is stored securely in the systems of The Service. The PUK is changed when the PINs associated with the private keys of the smart card are initially set by the Subscriber. PINs are set by the subscriber in the process when receiving the smart card (private keys). The subscriber uses the PIN related to a private key to activate it.
	Smart card, temporary	The smart cards are manufactured with a known default PUK. The PUK of the smart card is changed when the smart card is personalized at the premises of the RA, or the premises of Pointsharp, with the subscriber present. The PUK is stored securely in the systems of The Service. PINs associated with the private keys of the smart card are set by the subscriber in the process when personalizing and receiving the smart card (private keys). The subscriber uses the PIN related to a private key to activate it.

Issuing CA	Key protection	Method of activation
	Smart card, derived	Derived certificates for smart cards can either be issued to smart cards provided by The Service or to smart cards issued by another issuer approved by The Service. For smart cards provided by another issuer the current PINs of the smart card are used and are associated with the private keys according to key usage. Smart cards provided by The Service are manufactured with a known default PUK. The PUK of the smart card is changed when the smart card is personalized during the certificate enrolment process initiated by the subscriber. The PUK is stored securely in the systems of The Service. PINs associated with the private keys of the smart card are set by the subscriber in the process when personalizing and receiving the smart card (private keys). The subscriber uses the PIN related to a private key to activate it.
	Hardware token	Hardware tokens are manufactured with a known default administration code such as PUK or SO key. The administration code is changed when the Hardware token is personalized at the premises of the RA, or at the premises of Pointsharp, with the subscriber present. The administration code is stored securely in the systems of The Service. The PIN associated with the private key of the Hardware token is set by the subscriber in the process when personalizing and receiving the token (private key). The subscriber uses the PIN related to the private key to activate it.
Pointsharp SweID Mobile 3 CA vX	Mobile app	The private keys of the soft token receding in the mobile app are created in the certificate enrolment process activated by the subscriber. In the same process, the subscriber sets the PINs related to the private keys of the soft token. The subscriber uses the PIN related to a private key to activate it.

6.2.9 Method of deactivating private key

The CAs' private issuer keys are deactivated, for example, by closing the server application using them, restarting the HSM or removing the HSM. The CAs' private keys are stored in secure containers of HSMs when not in use.

Subscribers are responsible for deactivating their private keys when not in use.
When a smart card or hardware token is used, for example logging off or closing the application will deactivate the private key.
In mobile devices, closing the app will deactivate the private key.

6.2.10 Method of destroying private key

CA private keys are destroyed in a process that ensures that there are no residual remainings of the keys that could lead to the reconstruction of a CA key. Only personnel in Trusted roles may destroy the private keys by using commands as described by the HSM manufacturer.
Backup copies of CA private keys will also be destroyed as part of the process.

If an HSM that has contained CA key material will permanently leave the protected CA environment, it will be destroyed. A reliable de-magnetizer or physical destruction is used when destroying the HSM.

Subscriber private keys are never available to The Service. Subscribers are responsible to destroy or otherwise prevent misuse of expired or deserted subscriber private keys in their possession.

6.2.11 Cryptographic module rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The Service will archive a copy of all issued certificates and the corresponding public keys. The archives will be retained at least five (5) years after the expiration of the last certificate issued by the CA.

6.3.2 Certificate operational validity periods and key pair usage validity periods

Certificates issued within The Service have maximum validity periods according to the following table.

Certificates	Validity period (maximum)
Root CA	25 years
Issuing CA	12 years
Smart card or hardware token subscriber	5 years
Mobile subscriber	3 years

The Service may retire its CA private keys before the end of their validity. If so, all RAs (customers) and subcontractors will be notified, and third parties will be notified by information published on the repository: https://repository.pointsharpsecurecloud.com.

6.4 Activation data

6.4.1 Activation data generation and installation

The subscriber uses his private keys with the help of activation data, which are entered on the keyboard of a workstation, the PIN pad of a card reader, on a mobile phone, or another device. PINs of at least six digits are used for activation of subscribers' private keys.

For generation of the activation data for subscribers' private keys, see section 6.2.8.

6.4.2 Activation data protection

For LoA4 subscriber certificates, subscriber activation data (PINs and PUK) is sent directly from the processing center to the home address of the subscriber. The activation data is printed in a tamper proof envelope to ensure that the data is protected from unauthorized access.

The subscriber smart card, containing the subscriber private keys, and the envelope with the activation data are never present at the same time in the mail service, or other parts of the processing center. Envelopes with the activation data is printed and sent two days after the smart card has left the processing center.

For information concerning activation data of private keys related to LoA3 certificates, see section 6.2.8.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Service operations are built in such a way that Trusted roles, according to section 5.2, can be separated. All actions within the systems are logged and all personnel are identified at the individual level and authenticated in accordance with section 5.2.3.

The above applies regardless of whether the personnel acts directly within the central premises of the operations or whether the personnel is part of an external RA function.

All databases with subscribers' personal data and other sensitive information are encrypted. Direct access to information within databases are limited to trusted persons within Pointsharp having a valid operational reason for such access.

6.5.2 Computer security rating

No stipulations.

6.6 Life cycle security controls

6.6.1 System development controls

A separate preproduction environment, that is equivalent to the production environment, is used to test all changes intended to be implemented in the production systems before being implemented there. This is done to minimize the possibility of interruptions in The Service when changes are made to the system software, hardware, or configurations.

Software development is separately tested in a test environment before every release of the software. Final tests of the software are then made in preproduction, in the context of The Service, before it is taken into production.

Security tests are done at least annually regarding software and hardware used within The Service. Test results, security tests results and operations information are continuously documented and actions are taken if needed.

6.6.2 Security management controls

Both automatic and manual monitoring of security-related configurations of CA systems, firewalls, routers, software and access control are in use. Risk based management processes are used for change management and to prevent system failure.

6.6.3 Life cycle security controls

No stipulations.

6.7 Network security controls

A strict segmentation of the networks is implemented between applications, HSMs, CA, databases, RAs, and other external networks. Sensitive communication is protected using point-to-point encryption and only specific ports are opened for specific networks and ip addresses to ensure a high security level. Proxy´s and software for scanning abnormality are used throughout the network.

6.8 Timestamping

Controls are implemented to ensure the synchronization and accuracy of clocks being used in the systems. Multiple NTP (Network Time Protocol) servers are used to synchronize time and time is traceable to UTC.

Certificates, CRLs, OCSP responses, signatures, logs, and other database entries will contain time and date information.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

All certificates issued within The Service are subject to the certificate profiles that are in use. PsPT maintains these certificate profiles. The Certificate and CRL specifications are available at the online repository in accordance with section 2.1.

7.1.1 Version number(s), certificate extensions, and algorithm object identifiers

See Certificate and CRL specifications.

7.1.2 Name forms

The Service will use distinguished names that are composed of standard attribute types, such as those identified in RFC 5280 ("Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile").

7.1.3 Name constraints

Name Constraints are not used.

7.1.4 Certificate policy object identifier

See Certificate and CRL specifications and section 1.2.

7.1.5 Usage of policy constraints extension

Policy Constraints are not used.

7.1.6 Policy qualifiers syntax and semantics

Subscriber certificates will include statements in the Policy Qualifier field of the certificate policies extension, see section 1.2.

7.1.7 Processing semantics for the critical certificate policies

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

The Service Issuing CAs will issue X.509 version 2 CRLs that conform to RFC5280. The Certificate and CRL specifications are available at the online repository in accordance with section 2.1.

7.2.2 CRL and CRL entry extensions

CRL extensions will be supported in accordance with RFC 5280.

7.3 OCSP profile

The Service will operate an OCSP service in accordance with RFC6960 ("X.509 Internet Public Key Infrastructure Online Certificate Status Protocol").

7.3.1 Version number(s)

The Service will support X.509 version 1 OCSP requests and responses.

7.3.2 OCSP extensions

The Service OCSP responders will only use OCSP extensions that conform to the extensions profile in RFC6960.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

On at least an annual basis, Pointsharp performs a compliance audit to assess that The Service complies with this CP and CPS and the Swedish eID Assurance Framework. Compliance with the Swedish eID Assurance Framework will be assessed based on Pointsharp commitments as described in the Pointsharp application(s) to DIGG. Pointsharp will use an external party for the entire audit or parts of the audit. The auditor reports to PsPT and Pointsharp Board. Pointsharp will also continuously make internal audits to ensure compliance.

The RAs are contractually bound to follow the regulations stated in the Customer Agreement, The RA Trust Framework, the RA Declaration of Compliance, and for applicable sections from this CP and CPS, see section 1.3.2. RAs must report the results of their annual internal audit to PsPT.

Before approving an RA to be a part of The Service, Pointsharp verifies the RAs compliancy with this CP and CPS, and The RA Trust Framework by reviewing the RA's declarations of compliance and by conducting an initial audit of the RA.
Pointsharp makes audits of RAs' compliancy with this CP and CPS and The RA Trust Framework by conducting annual samples for a selection of RAs and by reviewing all RAs' annual internal audits and RAs' declarations of compliance.

8.2 Identity/qualifications of assessor

For internal audits on The Service conducted by an external auditor the requirements on the auditor are to be a qualified auditor of The RA Trust Framework.

General requirements on personnel performing audits and other assessments:

1. The scope of the audit or the assessment must be within the expertise of the personnel,
2. Must have a documented knowledge of Identity Assurance practices and PKI standards and implementations,
3. Must have a general knowledge of Pointsharp eIDs,

4. Must be trained and skilled in the auditing or assessment of secure information systems,
5. Must be familiar with compliance to trust frameworks, Information security management systems and IT, Internet and network security,
6. Must have a reputation for conducting its auditing and assessment business competently and correctly,

8.3 Assessor's relationship to assessed entity

An independent auditor will be used for the compliance audit, where independent means that the auditor is not involved in the daily operations and management of The Service.
The auditor must not have any major financial interest, or course of dealing that could foreseeably create a significant bias for or against Pointsharp and The Service including subcontractors.

Auditors of subcontractors and RAs will be appointed by Pointsharp and must not have any major financial interest, or course of dealing that could foreseeably create a significant bias for or against the audited party.

8.4 Topics covered by assessment

The main purpose of compliance audits are to verify that all routines and processes used for the issuing and lifecycle management of Net iD SweID certificates comply with:

1. Pointsharp's declaration of compliance in the DIGG license agreement for Swedish eIDs and the Swedish eID Assurance Framework.
2. This CP and CPS
3. RAs' compliance to The RA Trust Framework and their Declaration of compliance

Compliance audits includes the operations at Pointsharp, subcontractors, and RAs.
The audits will cover all requirements that define the operations of CAs and RAs under this CP and CPS. This includes but are not limited to:

1. The CA production integrity (key and certificate life cycle management),
2. CA and RA environmental controls,
3. CA and RA operational routines and processes,
4. This CP and CPS consistency with the Swedish eID Assurance Framework,
5. Signed agreements and other information that applies to Pointsharp's relations with RAs.

PsPT continuously conducts audits to ensure compliance to this CP and CPS, and frameworks as stated above. PsPT has the right to demand that subcontractors and RAs taking part in The Service operations take action on flaws found during audit in order to continue operating within The Service.

8.5 Actions taken as a result of deficiency

Information about deficiencies in The Service may come to the notice of PsPT through audits or via other sources in the daily operations, for example from employees,

subcontractors, or RAs. All parties that takes part in the operations of The Service are obliged to report any deficiencies as soon as possible when found.

PsPT is responsible for acting upon the flaws and faults discovered.
The measures taken must be adequate related to risk assessments made.
When PsPT identifies deficiencies in The Service operations, including subcontractors and RAs, all parties must act in accordance with PsPT's guidelines to update its routines.

Should this CP and CPS be updated in such a way that the new CP and CPS is deemed to involve a change of security or assurance levels, a new CP and CPS with a new identity will be created, see section 1.2 for OIDs.
After receiving a compliance audit report, or the annual internal audit report, concerning an RA, PsPT will contact the audited RA to discuss any exceptions or deficiencies shown by the audit. The audited RA and PsPT will, in good faith, use commercially reasonable efforts to agree on a corrective action plan to rectify the problems causing the exceptions or deficiencies and to implement the plan.

In the event of the audited entities failure to develop such a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that PsPT believe pose an immediate threat to the security or integrity of The Service, then:

1. PsPT will determine whether revocation and compromise reporting is necessary,
2. PsPT will be entitled to suspend services to the audited RA, and
3. If necessary, PsPT will terminate such services subject to this CP and CPS and the terms of the audited RA's contract.

8.6 Communication of results

The Auditor must provide PsPT with the results of the Compliance Audit for review, approval and to decide upon recommended actions.
The results will also, depending on scope of the audit, be communicated to Pointsharp Board, Pointsharp Management, and entities entitled by law, regulation, or agreement to receive a copy of the audit results.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Any fees associated with The Service will be regulated in the Customer Agreements.

9.1.1 Certificate issuance or renewal fees

According to section 9.1.

9.1.2 Certificate access fees

According to section 9.1.

9.1.3 Revocation or status information access fees

According to section 9.1.

9.1.4 Fees for other services

According to section 9.1.

9.1.5 Refund policy

According to section 9.1.

9.2 Financial responsibility

9.2.1 Insurance coverage

Pointsharp, subcontractors, and RAs must maintain a commercially reasonable level of insurance coverage its business covering for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or self-insured retention.

9.2.2 Other assets

Pointsharp will maintain, at its own expense, the insurance necessary to support its business practices.

Subcontractors and RAs must have sufficient financial resources to maintain their operations and perform their duties, in connectrion with The Service and they must be reasonably able to bear the risk of liability to subscribers and relying parties.

9.2.3 Insurance or warranty coverage for end-entities

No stipulations.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Information that is not explicitly or by other means defined as public in this CP and CPS is treated as confidential and is not given access to without an explicit agreement with Pointsharp.

9.3.2 Information not within the scope of confidential information

The following information is considered as public information:

- issued certificates including associated public keys
- revocation lists (CRLs) and OCSP responses
- this CP and CPS, The RA Trust Framework, and other regulatory documents published at https://repository.pointsharpsecurecloud.com.

Exceptions can apply for information related to specific RA organizations if this is formally agreed upon between Pointsharp and the RA.

9.3.3 Responsibility to protect confidential information

Pointsharp personnel, subcontractors, processing center, and RAs are responsible for protecting confidential information in accordance with this CP and CPS.

Combination of physical, logical and procedural security measures is used to protect all confidential information from unauthorized viewing, modification, or deletion.

9.4 Privacy of personal information

9.4.1 Privacy plan

The privacy processes and implementations of The Service is in accordance with the European general data protection regulation (EU) 2016/679, hereinafter referred to as the GDPR.

Pointsharp is acting as Personal data controller for personal data of subscribers being part of the Pointsharp organization or being involved in The Service operations and having a relationship to Pointsharp, either as employees, subcontractors, consultants or other contractual relationship.

Pointsharp is acting as a Personal data processor for the customer organizations (RAs) and is responsible for the protection of the RA subscribers' personal data within the systems of The Service according to Personal data processing agreements with the RAs. RAs must have their own privacy policies that conforms to the GDPR and are responsible for the management of their subscribers' personal data.
Pointsharp will assist the RAs, regarding their obligations as Personal data controllers with respect to the subscribers' "user rights" as stated in the GDPR.

Pointsharp has Personal data processing agreements with all subcontractors and the processing center and they must have privacy plans in place that conform to the GDPR.

All personnel involved with The Service are expected to handle personnel information in strict confidence and meet the requirements of the national (Swedish) law and European law concerning the protection of personal data. The Service participants must securely store and protect sensitive data against accidental or intentional disclosure.

The Service participants must not disclose or sell the names of certificate applicants or other identifying information about them, subject to section 9.3.2.

9.4.2 Information treated as private

Pointsharp will process personal data in connection with a subscriber's use of The Service. Any information about subscribers, including such subscriber's personal data, that is not made available to a relying party through the subscriber's own use of the subscriber certificate is treated as private and will not be transferred to any third party.

9.4.3 Information not deemed private

Information disclosed through certificate status services is not considered private information. The information not deemed private may include personal data. Such

personal data will be made public and shared with third parties in accordance with the privacy notice of The Service, available at https://www.pointsharp.com/privacy-notice.

9.4.4 Responsibility to protect private information

Participants in The Service processing private information must process such personal data in a secure manner and in accordance with what is stated in any instructions from the data controller and otherwise in accordance with applicable laws.

9.4.5 Notice and consent to use private information

Personal data shall only be processed by Pointsharp when there is a legal ground to do so and in accordance with what is stated in the privacy notice of The Service, available at https://www.pointsharp.com/privacy-notice.

9.4.6 Disclosure pursuant to judicial or administrative process

Pointsharp may disclose private information, without notice, when required to do so by law, regulation, or other requirements in this CP and CPS.
All disclosure must be made in accordance with applicable laws.

9.4.7 Other information disclosure circumstances

Pointsharp will not disclose any information containing personal data except for what is stated in section 9.4.3 and section 9.4.6.

9.5 Intellectual property rights

The allocation of intellectual property rights among participants in The Service, other than subscribers and relying parties, will be governed by the applicable agreements between such participants.

Subscriber's private and public keys are the property of the subscribers who rightfully hold them.

No part of this CP and CPS may be reproduced, published in a database system or transmitted in any form (electronic, mechanical, photocopied, recorded or similar) without written permission from Pointsharp AB. However, permission generally applies for reproducing and disseminating this CP and CPS in its entirety provided that this is at no charge and that no information in the document is added to, removed or changed.
Applications to reproduce and disseminate parts of this document in any other way may be made to Pointsharp in accordance with section 1.5.1.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Pointsharp will operate The Service in accordance with this CP and CPS and all other stipulations referenced in this document.
Pointsharp has as CA the overall responsibility for certificates issued within The Service and is acting as a Service RA for central RA tasks. Registration responsibilities for

subscriber certificates, however, are transferred to RA organizations (customer organizations acting as RAs in their RA domains) through Customer Agreements. Pointsharp requires that all organizations acting in the role as RA comply with all relevant provisions in this CP and CPS.

All certificates issued within The Service will include a reference to the relevant policy (OID) according to this CP and CPS.

All CA personnel will be authenticated with certificates issued via LoA4 issuing processes, issued within The Service, when performing actions in the CA applications. Audit logs and automatic log analyzing tools are the main controls in validating that unauthorized actions have not been undertaken. CA personnel is thereby individually accountable for the actions they perform.

Subscriber agreements may include additional representations and warranties.

9.6.2 RA representations and warranties

Pointsharp requires all Registration Authorities (RAs) acting on behalf of The Service to comply with the relevant provisions of The RA Trust Framework, this CP and CPS, and the Customer Agreement.

All RA personnel will be authenticated with certificates, issued by The Service, when performing actions in the CA applications, see section 3.2.5. Audit logs and automatic log analyzing tools are the main controls in validating that unauthorized actions have not been undertaken. RA personnel is thereby individually accountable for the actions they perform.

Subscriber agreements may include additional representations and warranties.

9.6.3 Subscriber representations and warranties

Pointsharp requires that subscribers ensure to comply with all the relevant provisions of this CP and CPS by accepting the Terms and Conditions of for the use of the e-identity prior to receiving certificates, smart cards, or other key bearers issued within The Service.
Subscribers shall further be required to protect their private keys, associated passwords and tokens, as applicable, and to take all reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.

Subscribers must only use the keys and certificates for the purposes identified in this CP and CPS and in any applicable agreement(s).

When a subscriber suspects a private key compromise, the subscriber must notify the RA representatives at the applicable RA, a Service RA representative, or a CA representative, in the manner specified in The RA Trust Framework and the RA Declaration of Compliance. When any other entity suspects private key compromise, they should notify RA or CA representatives.

9.6.4 Relying party representations and warranties

No stipulations.

9.6.5 Representations and warranties of other participants

No stipulations.

9.7 Disclaimers of warranties

Pointsharp disclaims all representations and warranties that are not explicitly mentioned in section 9.6.1 or in any other agreements or terms entered into with each applicable customer.

9.8 Limitations of liability

Pointsharp must not be held liable if subscribers, relying parties, or other entities using The Service in contradiction with The Service's terms and conditions of use for the certificates, this CP and CPS, The RA Trust Framework, Customer Agreements, or any other stipulations referenced in these documentation.

9.9 Indemnities

Indemnities may be regulated in the Customer Agreements, and the PoSC Net iD SweID Subscriber Agreement.

9.10 Term and termination

9.10.1 Term

This CP and CPS and any amendments are effective according to the effective dates set forth in conjunction with the publication of the CP and CPS to the repository of The Service, see section 2.1.
Each CP and CPS remains in effect until terminated or replaced by a newer version.

9.10.2 Termination

This CP and CPS will be terminated upon publication of a newer version or replacement document, or upon the termination of CA operations.

Notification regarding termination of the CA operations will be published no less than one (1) year in advance.

9.10.3 Effect of termination and survival

Upon termination of this CP and CPS, participants and subscribers of The Service shall still be bound by the terms for each issued certificate for the remainder of the certificate's validity period.
Responsibilities related to audit logs, archiving and the protection of confidential information will survive termination.
Upon termination, Pointsharp may communicate additional conditions and effects of the termination.

9.11 Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, participants in The Service will use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.
Notices are deemed effective after the sender has received an acknowledgment from Pointsharp.

9.12 Amendments

9.12.1 Procedure for amendment

PsPT determines what amendments should be made to this CP and CPS. Controls are in place to ensure that this CP and CPS is not amended and published without the prior authorization of PsPT. PsPT reviews this CP and CPS when necessary but at least annually.
Amendments to this CP or a CPS are posted to the online repository.

9.12.2 Notification mechanism and period

Pointsharp will notify participants upon significant changes to this CP and CPS at least one month before such changes are implemented. The participants will be notified in one of the following ways:

- Publications on the repository website; https://repository.pointsharpsecurecloud.com
- Communication directly with customer organizations (RAs)
- Communication directly with DIGG regarding the changes.

Pointsharp may, without notice, make editorial and typographical corrections and other changes that do not materially impact the participants in The Service.
Pointsharp does not have a fixed notification period for corrections.

9.12.3 Circumstances under which OID must be changed

If Pointsharp determines that an amendment to this CP and CPS necessitates a change in OID, then the revised version of the CP and CPS will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13 Dispute resolution provisions

Before resorting to any dispute resolution mechanism the disputing party must notify Pointsharp of the dispute with a view to seeking dispute resolution.
If a dispute arises regarding the interpretation or application of this CP and CPS, and the parties are unable to agree, the dispute shall be decided by the Ordinary Court in Sweden if not stated otherwise in a Customer Agreement between Pointsharp and the other applicable party, Swedish law must apply to the interpretation of this CP and CPS.

9.14 Governing law

Swedish law must govern the interpretation, construction, enforcement, and validity of agreements relating to this CP and CPS.

9.15 Compliance with applicable law

This CP and CPS is subject to Swedish law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

See section 1.1 for the Customer Agreement.

9.16.2 Assignment

See section 1.1.

9.16.3 Severability

No stipulations.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulations.

9.16.5 Force majeure

Pointsharp is not liable for a delay or failure to perform any obligation under this CP and CPS to the extent that the delay or failure is caused by events beyond what Pointsharp reasonably can control.
For example, the operation of the Internet is beyond what Pointsharp reasonably can control.

For customers having a Customer Agreement force majeure is regulated in the agreement.

9.17 Other provisions

No stipulations.

10 Appendix A Definitions and acronyms

Term	Synonym	Definition	Comment	Deprecated term
AD	active directory	Windows OS directory service that facilitates working with interconnected, complex and different network resources in a unified manner		
AIA	authority information access	link to the CA certificate of the certificate issuer		
ARL	authority revocation list	CRL with revocation information regarding CA certificates		
assymetric encryption	public-key cryptography	krypteringssystem där olika nycklar används för kryptering respektive dekryptering		
CA	certification authority certificate authority	certifies the ownership of a public key by the named subject of the certificate	In PoSC Net iD, Pointsharp acts as a CA for the issuing of e-identities within the PoSC Net iD.	
CP	certificate policy	document that describes the conditions under which a digital certificate may be issued and managed by a CA	State what are the different entities involved in the issuing, their roles, and their duties.	
CPS	certification practice statement	document from a CA which describes their practice for issuing and managing certificates according to the conditions in a CP		
CRL	certificate revocation list	signed list of certificate serial numbers of digital certificates that have been revoked by the issuing CA before their scheduled expiration date and should no longer be trusted		

Term	Synonym	Definition	Comment	Deprecated term
DIGG	Agency for Digital Government Myndigheten för digital förvaltning	Swedish authority responsible for the digitalisation of Sweden to achieve a sustainable welfare society together with the entire public administration		
digital certificate	certificate	electronic attachment that allows a person, computer or organization to exchange information securely over computer networks using the public key infrastructure (PKI)		
digital signature		digital code, generated and authenticated by public key encryption, which is attached to an electronically transmitted document to verify its contents and the sender's identity	Somewhat simplified, the digital signature can be considered as an electronic signature. The digital signature is a hash code.	
e-identity	electronic identity eID	a means for people to prove electronically that they are who they say they are and thus gain access to services	digital identity document based on X.509 v3 certificates and the use of private and public keys (PKI)	e-id eid e-ID
EUID	European Unique Identifier	identifier that comprises a country code, the register identifier, the registration number, and possibly a verification digit to enable the identification of companies and their branches in EU member states in the Business Registers Interconnection System		
GDPR	general data protection regulation	EU privacy and security law to protect the personal data of EU citizens		

Term	Synonym	Definition	Comment	Deprecated term
hardware token		small device, such as a smart card or USB flash drive that contains a small amount of storage holding a private key and a certificate		
HSM	hardware security module	physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication, and other cryptographic functions		
IdP	identity provider	system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying applications within a federation or distributed network		
ISMS	information security management system	defines and manages controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, availability, and integrity of assets from threats and vulnerabilities		
ISO/IEC	international organization for standardization/ international electrotechnical commission	technical standards issued by a joint technical committee (JTC) of ISO and IEC.	Its purpose is to develop, maintain and promote standards in the fields of information and communications technology (ICT).	

Term	Synonym	Definition	Comment	Deprecated term
key bearer		smart card, hardware token, mobile app, TPM, or other device used for storage and protection of the private keys of the Subcribers		
LoA	identity level of assurance	certainty with which a claim to a particular identity during authentication can be trusted to actually be the claimant's true identity	There are four, 1–4, levels of identity assurance. DIGG defines the levels 2–4 for Sweden.	
OCSP	online certificate status protocol	internet protocol used to get the revocation status of an X.509 digital certificate	To check that the token is valid and not withdrawn.	
OID	object identifier	identifier mechanism standardized by the International Telecommunications Union (ITU) and ISO/IEC for naming any object, concept, or "thing" with a globally unambiguous persistent name	http://www.oid-info.com/	
PIN	personal identification number	numeric passcode used by the subscriber to unlock the use of the private key within a token for the purpose of authentication, signing, or encryption		
PKI	public key infrastructure	set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption	PKI allows users of the internet and other public networks to engage in secure communication, data exchange, and money exchange through public and private cryptographic key pairs provided by a certificate authority.	

Term	Synonym	Definition	Comment	Deprecated term
PoSC ID		internal identification number created by the PoSC Net iD service and added to the subscriber certificate		
private key		digital cryptographic key that is used in pair with a public key in a PKI for		
PsPT	Pointsharp service Policy Team	entity at Pointsharp responsible for the regulatory frameworks of the PoSC Net iD and to uphold the compliance to the frameworks at Pointsharp, subcontractors, and RAs		
public key		digital cryptographic key that is used in pair with a private key in a PKI to prove the possession of the private key		
PUK	personal unblocking key	code used to reset a PIN that has been lost or forgotten		

Term	Synonym	Definition	Comment	Deprecated term
RA	registration authority	authority in a network that verifies user requests for a digital certificate and tells the certificate authority to issue it	RA is responsible for the following certification functions: • the identification and authentication of certificate applicants • the approval or rejection of certificate applications • initiating certificate revocations • processing subscriber requests to revoke or suspend their certificates. Refers to customer organizations that perform enrollment procedures for subscriber certificate applications within their RA domain. RAs operate under the terms and conditions of the customer agreement and this CP and CPS,	
RA Officer		individual at an RA that administers subscribers, key bearers, and certificates		
relying party		RA organization with a valid customer agreement for the PoSC Net iD, or any other organization, person, application, or device that uses subscriber certificates issued by PoSC Net iD		
security incident		event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed		

Term	Synonym	Definition	Comment	Deprecated term
separation of duties	segregation of duties SOD multi-person control duality	internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task	At least two people are required to perform the action. This is for security reasons. Separation of duties may be enforced electronically or by manual procedures or both. Sensitive tasks require the collaboration of multiple persons in Trusted roles. At least the tasks will only be allowed to be performed with multi-person control ("n" out of "m"), where "n" needs to be at least 2 persons.	
Service RA	PoSC Net iD RA	central RA function within PoSC Net iD	Operated by Pointsharp.	
sign-up preparation form		document given to new customers asking for necessary information so that Pointsharp can register and validate the customer		
smart card	chip card integrated circuit card (ICC)	card with a built-in microprocessor that can be used to protect private keys of a subscriber		
smart card reader	card reader	device used for communication with a smart card or a memory card		
soft token	software token	two-factor authentication security device that may be used to authorize the use of computer services		

Term	Synonym	Definition	Comment	Deprecated term
SPAR	statens personadress register	Swedish tax authority's national register of citizens and other residents with a Swedish personal identification number or a Swedish coordination number		
SSO	single sign-on	authentication process that allows a user to access multiple applications with one set of login credentials		
subscriber	end-user	individual applying for or using an e-identity (certificate)		
subscriber agreement	subscriber terms and conditions	terms and conditions for the use of an e-identity		
symmetric encryption		encryption where the same encryption key is used both to encrypt and decrypt data		
trusted certificate				
UPS	uninterruptible power supply	electrical apparatus that provides emergency power to a load when the input power source or mains power fails		
USB Token	hardware token	USB hardware with a built-in smart card		

Term	Synonym	Definition	Comment	Deprecated term
VAT identification number	value added tax identification number	individual number given to each taxable person intending to make supplies of goods or services, or to make acquisitions of goods for business purposes, each number having a prefix of two letters by which the Member State of issue is identified		
WSDL	web services description language	XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information	The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate. However, the only bindings described in this document describe how to use WSDL in conjunction with SOAP 1.1, HTTP GET/POST, and MIME.	
YubiKey		hardware token from Yubico	The part used for the e-identity is based on PIV standards.	

Website
https://www.pointsharp.com

Disclaimer
Specifications subject to change without further notice, unless stated otherwise in agreement.

Classification:	Public
Publ. No.:	PSC-Rd22-01
Document version:	1.2
Document status:	Final
OID:	1.2.752.179.100.2.3
Published:	29 Sep 2023