AB Svenska Pass CA Class1 v1

Certificate Policy

Certification Practice Statement

V 2.0

OID 1.2.752.244.1.2.2
Date 2020-08-31
Version 2.0
Document owned by: AB Svenska Pass Trusted Services Management Board

Document change history

V 1.0 13/1/2017	Initial document
V 1.1 25/1/2019	- Spelling, grammatical corrections and editorial changes all over the document - 1.1: Mention the compliance to Swedish Trust framework for Swedish eID and inspiration from ETSI EN 319411 part 1 - 1.2: correction of the CPS OID - 1.3.1: correction of the CA contact info and add description of the different CAs - 1.3.2: clarification of RA - 1.3.5: mention Conapto as other participant - 1.5.4: correction of the VA link - 2.1: add rootCA crl link - 2.2: mention the CRL as a revocation information - 3.1: clarify givenname and replace it by First name - 3.2.1: mention that the keys can be generated in a secure environment - 3.2.2: clarification of individual identity authentication - 3.4: clarification of revocation request authentication - 4.9.3: clarification of revocation request - 5: add section description - 5.1: clarification of physical controls - 5.2: clarification of procedural controls - 5.3: clarification of personal controls - 5.3.6: Mention the sanctions for unauthorized actions - 5.3.7: Mention the independent contractor requirements - 5.4.1: correct the type of events recorded - 5.4.3: clarification of log retention period - 5.4.4: corrects title - 5.4.8: mention the log vulnerability assessment - 5.5: correct and add descriptions for records archival - 5.5.1: correct the type of record archived - 5.6: clarification of key changeover - 5.7: clarification of Compromise and disaster recovery - 5.8: clarification of CA/RA termination - 6.1: clarification of key pair generation and installation - 6.1.5: correction of the key sizes - 6.2: clarification of the private key protection - 6.3: add description for other aspects of key pair management - 6.4: clarification of activation data - 6.6: clarification of life cycle technical controls - 6.7: clarification of network security controls - 6.8: clarification of time stamping - 7.1.3: add description for the cryptographic algorithm OID - 8: add description for compliance audit - 8.1: mention that the audit can be conducted by an external entity - 9.4: add description for privacy of personal information - 9.4.2: clarification of the information considered as private

	- 9.6.4: mention that certificate chain should be uploaded from the repository by the relying party - 9.12.2: clarification of the notification period for amendment process
V1.2 29/06/2020	- Spelling, grammatical corrections and editorial changes all over the document - Change the name of Gemalto Company to Thales DIS all over the document - Clarify that the used cards are SSCD type all over the document - 1, 1.1- 8- 8.4: Mention the compliance to Swedish Trust framework for Swedish eID - level 3 - 1.3.1: Update the address of Thales DIS the CA company - 6.1-6.2: Remove the card description
V2.0 XX/09/2020	- 1, 1.1, 8, 8.4: change the compliance to Swedish Trust framework for Swedish eID - level 4 - 1.2: change the CPS OID - Update the eID cards from SSCD to QSCD type - 6.1-6.2: add new card description

Table of Contents

1 Introduction

This document defines the Certificate Policy (CP) and Certification Practice Statement (CPS), hereinafter referred to as “CP/CPS” applicable to the e-ID certificates issued by the “AB Svenska Pass PKI“ within level 4 according to the Trust framework of Swedish e-ID [2].

AB Svenska Pass will create authentication and “digital signature” certificates, for its subscriber, issued under AB Svenska Pass iCA Class1 v1. The private keys connected to these certificates will be stored in a QSCD. The iCA is part of the “AB Svenska Pass Trusted Services" (ABSP-TS).

This document is produced for subscribers, relying parties, bodies responsible for accreditation or supervision, and everyone with an interest in how the e-IDs issued by AB Svenska Pass works. It states the obligations AB Svenska Pass has and details the processes AB Svenska Pass follows within ABSP-TS and its Certification Authorities (CAs). This document takes into consideration the AB Svenska Pass Root CA Class1 v1 and the subordinated issuing CA, AB Svenska Pass iCA Class1 v1.

AB Svenska Pass CA Class1 v1 CP/CPS conforms to the structure detailed in “X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” (RFC 3647).

1.1 Overview

This CP/CPS defines security requirements, procedures and routines that AB Svenska Pass, as issuer of the AB Svenska Pass e-ID, applies when producing eID certificates mainly conform to the Swedish Trust framework for Swedish eID [2]-level 4. Practices described in this CP/CPS are also inspired from ETSI EN 319411 part 1[3] for certificates for digital identification and encryption. These certificates are used in ID-Cards issued by Swedish governmental agencies, where these ID Cards are equipped with an approved QSCD.

This CP/CPS describes the valid processes used through the full lifecycle of the Certificates, including issuing certificates for card-holders revocation and validation checks.

Parts of the provided services may be performed by a subcontractor or other parties. For instance the RA function is always performed by an issuer of highly trusted physical ID Cards. Nevertheless AB Svenska Pass will always be held ultimately responsible for the eID in accordance with this CP/CPS.

1.2 Document name and identification

The routines and roles resulting from this CP/CPS apply only in connection with certificates referring to “AB Svenska Pass iCA Class1 v1“.

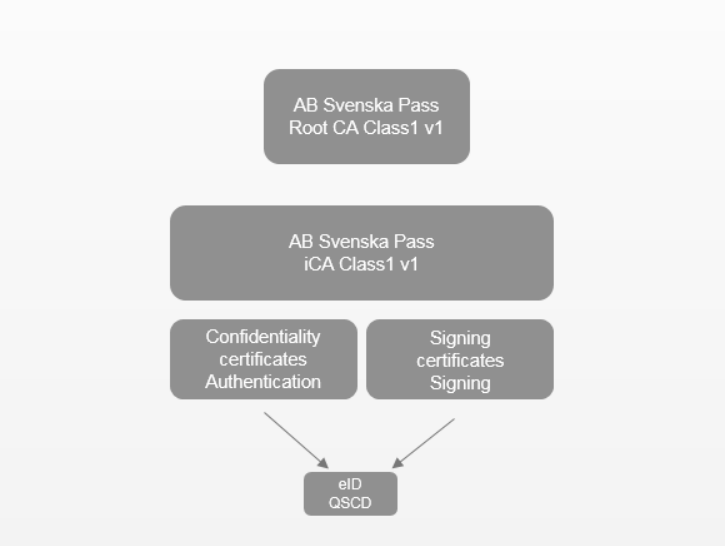
The name of this CP/CPS is AB Svenska Pass CA Certificate Practice Statement and the object identifier is 1.2.752.244.1.2.2

1.3 PKI participants

AB Svenska Pass issues AB Svenska Pass e-ID to holders of highly trusted ID Cards, issued by Swedish governmental agencies.

1.3.1 CA

The scope of this CPS document includes the Root CA (RCA) and iCA of AB Svenska Pass CA Class1 v1. The RCA issues certificates to the iCA and the iCA issues certificates for e-ID use. The iCA issues two certificate types, one for authentication and the other for digital signatures. The authentication certificate can be used for authentication of a person's identity, log-in processes or authentication to signing services, while the signing certificate is used for signing.



AB Svenska Pass operates the CAs that acts according to this CP/CPS and will ensure that all required recourses are available to meet its obligations.

AB Svenska Pass is a fully owned subsidiary of Thales DIS Sweden AB.

Thales DIS Sweden AB
Glasfibergatan 12

svenskapass.CAinfo@gemalto.com
www.thalesgroup.com

- AB Svenska Pass **Root CA:**

AB Svenska Pass Root CA is the first level CA constituting the basis of trust for the entire PKI architecture. It is a self-signed CA which issues certificates to the subordinate CAs.
AB Svenska Pass Root CA is an offline CA and don't issue certificates to end users.
AB Svenska Pass Root CA's tasks are:

- Issue and manage the subordinate CA certificate (iCA) life cycles.
- Generate and publish ARLs periodically and after a CA certificate revocation.
- Issue and manage this CP/CPS
- Ensure adherence to the CP/CPS
- Publish the CA certificates issued by the Root CA.

- **Subordinate CAs**

Subordinate CAs are issued by the AB Svenska Pass Root CA and are used to issue and manage eID certificates life cycles.
Subordinate CA's tasks are:

- Issue and manage eID certificates life cycle.
- Generate and publish CRLs periodically and after an end user certificate revocation.
- Ensure adherence to this CP/CPS
- Publish the eID certificates issued by the subordinate CA.

The AB Svenska Pass PKI architecture contains the following subordinate CAs

- **Issuing CA:**

This CA issues the following certificates profiles:

- Authentication
- Digital Signature
- Encryption

1.3.2 RA

Swedish governmental agencies that issue highly trusted ID, and are appointed by AB Svenska Pass, to act as a Registration Authority (RA) for Certificates issued by the iCA.

This part of the process is done by the Swedish authority, but responsibility to the Swedish E-Identification Board and its regulations, resides with AB Svenska Pass as issuer of the eID. Responsibility and allocation of roles is documented and agreed between the parties.

Registration authorities' tasks are to:

- Establish enrollment procedures for eID certificate applicants,
- Perform identification and authentication of certificate applicants,
- Initiate or pass along revocation/suspension requests for certificates, and
- Approve applications for renewal or re-keying certificates.

1.3.3 Subscribers

A subscriber must be a card holder of a highly trusted ID card, issued by a Swedish governmental agency.

All subscribers must sign an approval contract containing AB Svenska Pass' conditions in order to use AB Svenska Pass e-ID.

The AB Svenska Pass e-ID is equipped with two certificates, a "digital signature certificate" for electronic signatures and an "authentication certificate" to be used for authentication and/or encryption services. The two certificates of the AB Svenska Pass e-ID are handled as one unit, for example regarding revocation both certificates are revoked if the physical card is subject to revocation.

1.3.4 Relying parties

Relying parties are entities who use ABSP PKI certificates to verify the identity of subscribers and/or digital signature with reference to a public key listed in a subscriber certificate.

1.3.5 Other participants

- **Conapto:**

Conapto provides hosting services for the CA service. This includes server racks, monitoring and hosting up to the OS level. Applications and HSMSs are operated by AB Svenska Pass. Conapto does not have physical or logical access to the HSMs.

1.4 Certificate usage

An approved application for AB Svenska Pass e-ID will generate two certificates for the subscriber to use. The "digital signature" certificate and its corresponding private key shall only be used in the creation of Electronic Signatures. The "authentication certificate" and its corresponding private key can be used for authentication/ identification and encryption/decryption purposes.

Both the "digital signature" certificate and "authentication" certificate are issued by "AB Svenska Pass Class1 iCA v1".

The subscriber of an AB Svenska Pass e-ID and its relying parties are legally bound through contractual agreements with AB Svenska Pass.

The appropriate key usage, included in the key usage extension of each certificate, indicate the certificate's usage are and must be taken into consideration when certificates, and their corresponding private keys are used.

It is out with AB Svenska Pass´ control to prevent private keys from being used for unwanted purposes or for purposes out with the subscriber's intentions. It is in the subscriber's interests and responsibility to use the private keys only in trustworthy applications and with reliable equipment. It is a common understanding that a subscriber never shall use the private signature key to sign data or documents that they have not first reviewed and approved.

1.5 Policy administration

1.5.1 Organization administering the document

AB Svenska Pass Trust Service Executive Board (ABSP.TSEB) operates within AB Svenska Pass and is responsible for the CP/CPS and certificate profiles of the overall Public Key Infrastructure (PKI). The board is responsible to ensure that this CP/CPS meets the requirements stated in 1.5 and that the issuance of the ABSP e-ID is done in accordance with this CP/CPS.

1.5.2 Contact person

Enquiries or other need for communications about this CP/CPS should be addressed to: ABSP_TSEB@gemalto.com

1.5.3 Person determining CP/CPS suitability for the policy

ABSP-TSEB has the duty to ensure the suitability of this CP/CPS.

1.5.4 CP/CPS approval procedures

The ABSP_TSEB is responsible for changes to this CP/CPS. The two types of possible change are to issuing a new CP/CPS or make changes to the existing CP/CPS.

The CP/CPS is published in PDF format on the web site: https://va.absvenskapass.se/CPS2.

AB Svenska Pass Executive Board will review any changes to this CP/CPS and is responsible to check that modifications, additions or deletions are in line with CP/CPS references (Appendix A), amendment procedure are defined in 9.12.

1.6 Definitions and acronyms

A list of definitions and acronyms can be found in Appendix A

2 Publication and Repository Responsibilities

2.1 Repositories

The AB Svenska Pass CP/CPS, CA certificates and revocation information is made available on AB Svenska Pass website:

https://va.absvenskapass.se/CPS2
http://va.absvenskapass.se/absvenskapass-class1-iCA-v1-2.crt
http://va.absvenskapass.se/absvenskapass-class1-rootCA-v1.crt
http://va.absvenskapass.se/absvenskapass-class1-iCA-v1.crl
http://va.absvenskapass.se/absvenskapass-class1-rootCA-v1.crl

2.2 Publication of certificate information

AB Svenska Pass will make the following information available:

- The CP/CPS.
- Issuing CA certificates.
- Root CA certificate
- Revocation information of certificates accessible via CRLs or via OCSP responders open to AB Svenska Pass and AB Svenska Pass relying parties with valid AB Svenska Pass relying party agreements.

The location of the repository and OCSP responders are given in certificate profiles, section 7.1.

2.3 Time or frequency of publication

Certificate information is published promptly after issuance and within 24 hours after revocation. The information is available 7 days per week, 24 hours per day, except when there is planned maintenance or other factors beyond the control of AB Svenska Pass. In case of interruptions in the services AB Svenska Pass will as soon as possible begin the work to restore the services to obtain normal functionality.

2.4 Access controls on repositories

Only AB Svenska Pass has write access to ABSP Repository Service. Relying parties have read-only access 7 days per week, 24 hours per day. Exceptions can be made for system maintenance.

3 Identification and Authentication

Face-to-face identity verification is required to assure the identity of the subscriber. AB Svenska Pass e-ID is only issued to card holders of highly trusted ID Cards issued by Swedish governmental agencies and equipped with an approved QSCD.

3.1 Naming

The subscriber is registered with identity, name and contact information. This will be performed by a RA appointed by AB Svenska Pass. The subscriber's personal identity number is used to unambiguously identify the subscriber.

The certificates in AB Svenska Pass e-ID will include subject distinguished names in accordance with the X.500 series of standards. The certificate subject name attributes and encoding are according to section 7.1.5. The following subscriber information is included in AB Svenska Pass e-ID certificates:

Information	Content
First Name	Subscriber´s first name
Surname	All of the subscriber's surnames spelled according to the register. Pseudonyms are not allowed.
Country	"SE", Sweden, the country where the subscriber is resident at the time of the certificate application.
Serial number	This field contains a valid personal identity number in the form "YYYYMMDD-NNNN"
Card serial number	The card serial number which uniquely identify a certain ID Card.

AB Svenska Pass is not obligated to look for evidence of trademarks by any organization.

3.2 Initial identity validation

Identity validation is in compliance with this CP/CPS and the certificate profile, detailed in section 7.1.

3.2.1 Method to prove possession of private key

The subscriber's private keys are generated in the chip of the QSCD or generated in a secure environment and injected into the card (QSCD).

The RA securely transfers the signed PKCS#10 or CRS (Certificate Request Syntax) request to AB Svenska Pass systems. The systems of AB Svenska Pass validate the authenticity and integrity of all RA requests.

The certificates are then issued by the CA systems and returned to the requesting RA to be stored in the corresponding card. The personalized card is then distributed by the issuer of the ID card to the subscriber, in a secure manner

3.2.2 Authentication of individual identity

Applications are submitted via a personal visit to the authority. The person that applies for eID must identify themselves with an approved ID document. All security details are checked in the ID and the validity of the ID. The applicant can also choose to support their identity by the RA comparing data in the application with data on a resident's permit that is registered with Migrationsverket (Migration Agency) according to 3a § directive (2009:284) on ID cards for people in the persons register in Sweden. If this is the case, the applicant must give their consent to the data required for the application to be obtained directly from the Migration Agency register. In the absence of an approved ID document, the applicants can identify themselves via an approved certifier that can identify themselves and certify the applicant's details.

To be a subscriber of AB Svenska Pass e-ID, an application must be filled in and signed by the individual applicant. Identification checks will be made by the issuer of the ID Card. AB Svenska Pass will keep a record of identification information used for the authentication of the individual for at least ten years after the expiration date of the issued AB Svenska Pass e-ID.

The authentication process will follow routines for issuing cards as national ID Cards from the police, highly trusted ID Cards issued by other Swedish governmental agencies. Before the AB Svenska Pass e-ID certificates are issued, the information in the application is checked against the Swedish national register SPAR or other register approved by AB Svenska Pass. In case the subscriber is under age of 18, permission has been received signed by all guardians.

3.2.3 Criteria for operation or interoperation

No cross certification will be undertaken by AB Svenska Pass within the scope of this CP/CPS.

3.3 Identification and authentication for re-key request

No re-key requests are permitted by AB Svenska Pass within the scope of this CP/CPS.

3.4 Identification and authentication for revocation request

A subscriber can request that an eID be revoked by making a phone call to the AB Svenska Pass revocation service. The subscriber has to provide necessary information in order for AB Svenska Pass to be able to revoke the certificates.

Any misuse of the AB Svenska Pass e-ID will permit the id-card, on behalf of the subscriber or based on its own legal rights, to revoke the eID.

The AB Svenska Pass administrator uses personal credentials to log-in to the revocation application. AB Svenska Pass will keep records of all revocation requests. The records will hold information of the identity of the subscriber, the identity of the administrator revoking the certificates and the time the revocation was performed. The records are included in the audit logs of the RA systems in AB Svenska Pass production facilities.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

An application for an AB Svenska Pass e-ID is made, in-person, by the applicant at a Swedish governmental agency. The application form and data is collected and processed by a RA administrator. The RA sends the application form and /or data to AB Svenska Pass.

4.1.1 Who can submit a certificate application

Application for an AB Svenska Pass e-ID is part of the application process for the physical ID Card. Registration information is collected by RA and sent to AB Svenska Pass.

4.1.2 Enrolment process and responsibilities

The application procedure is done at the authority with a personal check of identity. This is done in accordance with DNV SPC151-U. The subscriber is bound through a subscriber agreement with AB Svenska Pass. The subscriber accepts the Terms and conditions for e-IDs from AB Svenska Pass (Villkor för AB Svenska Pass e-ID) at the time of application for the AB Svenska Pass e-ID.

4.2 Certificate application processing

4.2.1 Approval or rejection of certificate applications

An RA, on behalf of AB Svenska Pass, will always identify the applicant and authenticate the AB Svenska Pass e-ID application.

When identification and authentication processes have been finished the RA creates a secured file of applications and sends it to AB Svenska Pass. The individual responsibility of RA administrators is governed by internal RA routines. The local access control routines create log files that always show who is responsible for processing each application. When AB Svenska Pass receives and validates the application files, certificate issuance will begin, according to section 4.3.

4.2.2 Time for processing certificate applications

AB Svenska Pass will approve an application for AB Svenska Pass e-ID if it meets the requirements of validation and authentication executed by an appointed RA and according to this CP/CPS. Delivery is performed according to the routines for the physical ID Cards.

4.3 Certificate issuance

AB Svenska Pass approves the application by issuing an AB Svenska Pass e-ID certificate and storing it in the QSCD of the physical ID card, which is issued at the same time

The production process for issuing AB Svenska Pass e-ID certificates with the private keys protected in the QSCD, consist of at least of the following activities:

- Authentication of application’s secure files submitted by the RA.

- Validation of the applicant's personal information against the SPAR register or other equivalent register approved by AB Svenska Pass.
- Key generation on cards (QSCD) or secure key generation and key injection to the card (QSCD)
- Certificate request, creation and storage of certificates on cards (QSCD).
- Creation of activation data, i.e. PUK code.
- Electronically personalization of cards.
- Distribution of activation data i.e. letter in secured envelopes with PUK code. The envelopes are temper proof and the content of the letters is impossible to view from the "outside".
- Distribution of the ID card with QSCD to the card issuer for secure physical delivery based on face-to-face identification.

Due to the principle on segregation of duties, no individual has the rights to perform all the steps mentioned above.

When the certificates have been issued, together with the corresponding ID card and its QSCD, the subscriber will be notified by the ID card issuer.

4.4 Certificate acceptance

By signing the application agreement and accepting delivery of the ID card with the QSCD that includes AB Svenska Pass e-ID certificate and corresponding private keys, the subscriber accepts to comply with all the obligations given in the application form.

4.5 Key pair and certificate usage

4.5.1 Subscriber's private key and certificate usage

The subscriber shall only use certificates and their associated key pairs for the purposes identified in this CP/CPS and in the agreement with AB Svenska Pass. The defined areas are described in subsection 1.4 and application labelling takes place in accordance with X.509 and chapter 7.

Subscribers must accept the subscriber agreement of AB Svenska Pass e-ID before receiving the ID card with the QSCD and the private keys corresponding to the subscriber. For more information regarding appropriate subscriber key usage see section 1.4.

4.5.2 Relying party public key and certificate usage

Prior to accepting AB Svenska Pass e-ID, a relying party is responsible for verifying that the certificates are appropriate for the intended use and check that they are valid, i.e. verify the validity dates and the validity of the certificate issuance signatures, key usage, including proper age for signing documents and the status of the certificate. The status of a user certificate must be validated only against production certificates available online:

http://va.absvenskapass.se/absvenskapass-class1-iCA-v1-2.crt
http://va.absvenskapass.se/absvenskapass-class1-rootCA-v1.crt

4.6 Certificate renewal

The CP/CPS does not support renewal of subscriber's certificates.

4.7 Certificate re-key

The CP/CPS does not support re-key services.

4.8 Certificate modification

The CP/CPS does not support certification modification.

4.9 Certificate revocation and suspension

The CP/CPS does not support suspension services.
Revocation will be carried out based on a request from the subscriber or in the case of any other event that requires revocation to take place.

4.9.1 Circumstances for revocation

There shall be no renewal of certificates. If there is a new request to AB Svenska Pass iCA Class1 v1, for the same subscriber within the life length of the certificate, the active certificate by AB Svenska Pass iCA Class 1 v1 will be revoked.

If the cardholder breaches the subscriber agreement, AB Svenska Pass has the right to revoke the eID and all related certificates. AB Svenska Pass may also revoke the eID if it discovers that it contains details that are incorrect or incomplete, or if there are reasons to suspect that this is the case; if it has been misused or there are reasons to suspect that it may be misused; or if AB Svenska Pass is obliged to act, as a result of legislation or the decision of a governmental authority. AB Svenska Pass may also revoke the eID and any certificate on behalf of a subscriber when presented with written consent.

AB Svenska Pass is entitled to recall all the eIDs that are connected to an issuer of ID cards if the agreement between AB Svenska Pass and the issuer to supply ID cards with eIDs is terminated. A recall of eIDs will always result in a revocation of the connected certificates.

The subscriber is obliged to immediately request revocation of the eID with its certificates if the card or security codes are lost, have been out of control of the subscriber, or if there is a suspicion that the identity could have been misused.

4.9.2 Who can request revocation

Revocation can be performed at any time following a request from subscriber. The RA and AB Svenska Pass also have the right to revoke an eID or a certificate under the circumstances stated in 4.9.1.

4.9.3 Procedures for revocation request

AB Svenska Pass provides a revocation service that is available 7 days per week, 24 hours per day. The subscriber will have to provide necessary information for the revocation service to execute the revocation. The subscriber personal data will be

asked for by the revocation service. The revocation shall be proceeded after it has been confirmed by AB Svenska Pass.

When a request to block comes by phone, the person calling can state their civil registration number. Here, ABSP considers what is most important to avoid risking a block NOT being implemented, due to an absence, knowledge etc., if alternative or additional control questions were required. Validation of the card can also be done via the same channel, in this case, the card number is required. A certificate revocation is permanent.

4.9.4 Revocation request grace period

There is no revocation grace period. The revocation request towards AB Svenska Pass revocation service shall be processed immediately without delay. Time within which the CA must process the revocation request

4.9.5 Time within which the CA must process the revocation request

AB Svenska Pass shall revoke AB Svenska Pass e-ID certificates promptly after receiving a valid revocation request.

4.9.6 Revocation checking requirement for relying parties

Prior to accepting an AB Svenska Pass e-ID certificate, a relying party is responsible to check the status of its certificate against the CRL or appropriate OCSP responder. If AB Svenska Pass OCSP responders, CRL or revocation services cannot be received due to system failure or similar, the certificates shall not be accepted.

AB Svenska Pass will provide certificate status information identifying the access point to the OCSP responders in every AB Svenska Pass e-ID certificate.
Relying parties should follow requirements in 4.5.2 to validate the eID certificate.

4.9.7 CRL issuance frequency

CRL’s are issued with a 1 day frequency.

4.9.8 On-line revocation/status checking availability

AB Svenska Pass provides revocation status checking using the OCSP protocol.
http://va.absvenskapass.se/ocsp

4.9.9 On-line revocation checking requirements

All responses will be signed by a private key, corresponding to a public key certified by the CA, to which the OCSP request is made.

4.10 Certificate status services

4.10.1 Operational characteristics

The address to the OCSP responders is:
Domain Name: va.absvenskapass.se/ocsp
Port number: 80

4.10.2 Service availability

The AB Svenska Pass OCSP responder is available 7 days per week, 24 hours per day except during planned maintenance.

4.11 End of subscription

The validity of subscriber certificates issued by the iCA is five (5) years. If a subscriber chooses to unsubscribe before this period, the certificates shall be revoked. When a subscriber revokes the certificates the procedures under 4.9 shall be followed.

4.12 Key escrow and recovery

Not applicable.

5 Facility, Management and Operational Controls

As a subsidiary company of Thales, information security work at AB Svenska Pass is governed by a central security policy, which not only addresses physical and IT security but also information security.

To implement the principles in this central security policy, Thales has defined a management system for security at company level that is based on a risk-based method according to ISO 27001.

5.1 Physical Controls

AB Svenska Pass CA has a national, dual site location. The RCA is stored offline. The sites are geographically spread. AB Svenska Pass, as well Conapto is certified according to the international standard on information security control, ISO 27001 [4] [5].

5.1.1 Site location and construction

AB Svenska Pass operates the PKI infrastructure in physically protected datacenters, located on two geographically spread sites. This datacenter is composed of different security zones and locked rooms, cages, safes, and cabinets with strict physical access.

5.1.2 Physical access

Physical access must be authorized by AB Svenska Pass and is only granted to a limited number of people. The physical areas are divided into security zones. Access is controlled by zone, and limited to people assigned to carry out a specific work in a particular zone. Strict access control is enforced in all areas containing highly sensitive material and infrastructure including material and infrastructure pertaining to signing certificates, CRL's, OCSP and archives.

All entries and other events are logged.

The Physical environment is secured by access control, mantraps and CCTV. Access to the physical environment is monitored 24/7. Surveillance is done by in house security personnel during working hours and by an external security company at other times.

Controls for natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc. are implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

5.1.3 Power and air conditioning

The AB Svenska Pass PKI data center secure zone is powered through a dual and uninterrupted power supply (UPS) units, to prevent shutdown or power failure. In the event of a power failure there is an automatic failover to a standby generator.

Secure zones are also equipped with air conditioning systems 24/7 to ensure constant temperature and humidity.

5.1.4 Water exposures

The AB Svenska Pass PKI takes reasonable precautions against water exposure to its secure zones.

5.1.5 Fire prevention and protection

The AB Svenska Pass PKI secure zone is equipped with smoke and heat detectors connected to the building's surveillance center.

5.1.6 Media storage

All magnetic media containing AB Svenska Pass PKI information are stored in a secure zone physically protected from fire and water damage. Media storage are located either within the AB Svenska Pass PKI primary site or in a secure off-site storage area. See 5.1.8

5.1.7 Waste disposal

Depending on the classification of the data, paper documents or magnetic media containing sensitive data are securely disposed of by:

- Shredding, or destruction of paper documents.
- Physical damage or destruction of magnetic media.

5.1.8 Off-site backup

AB Svenska Pass PKI maintains a disaster recovery site located in Stockholm NORTH from where PKI services can be resumed in case of an emergency and loss of sensitive PKI data. The off-site has appropriate levels of physical security the same as described in 5.1.

5.2 Procedural Controls

5.2.1 Trusted roles

The CA organization contains of a set of trusted roles. Members of each role have specific functions and rights to carry out specific activities. Only personnel that have been controlled and meet specific security requirements can have a trusted role in the AB Svenska Pass CA Organization. Access to systems that results a certificate generation, are controlled in a way that no one alone should be able to have access to the CA system and its functions.
Trusted roles defined in this CP/CPS are:
Trust Service Director*: Can delegate and revoke role personnel and responsibilities. Responsible for compliance with security procedures and rules. Responsible for a key component.*
Local security manager Responsible of the development and application of the security policy within the AB Svenska Pass PKI.
Security Officer: Access to private key material. Can reinstall HSM. Can perform backups and configuration of HSM.
Operator: Administration of HSMs and EJBCA application. Can renew and generate keys.

Auditor: Authorized to view archives and audit logs of the RCA trustworthy systems. Are responsible of conducting internal and external audits in a regular time interval as defined in 8. The audit reference is mainly this CP/CPS in addition to other related manuals and procedures such as the security policy.

Every person that has a trusted role in the organization has been background checked, according to the internal AB Svenska Pass personnel process. It is also ensured that personnel do not have any other position in the organization that might conflict with their trusted CA role.

5.2.2 Number of persons required per task

Critical actions in the PKI, such as CA certificate issuing, revocation or CA keys activation deactivation destruction in the HSM, should be performed by at least *two persons*.
The m of n rule is used to administrate HSMs. At least:

- *2* out of *3* persons are needed to activate a CA key
- *2* out of *3* persons are needed to revoke a CA key
- Key ceremonies - Generating and managing keys requires several different roles to maintain security

eID certificate generation and revocation tasks are performed by two persons.

5.2.3 Identification and authentication for each role

In addition to the physical access controls, AB Svenska Pass PKI implements identification and authentication controls for personnel fulfilling trusted roles. They are identified to CA systems and HSMs using authentication certificates stored in tokens or smartcards.
Login and password can be also used for less critical systems and services.

5.2.4 Roles requiring separation of duties

To reduce opportunities for unauthorized or unintentional modification or misuse of the PKI assets, at least two persons are required to satisfy a trusted function in the CA. By splitting the task, each person provides its separate part of knowledge on the task. The separate roles are configured automatically on the CA systems. For example if a person is logged as an auditor, he can never be logged as CA/RA operator with the same credentials.

5.3 Personal Controls

AB Svenska Pass implements certain security controls with regard to the duties and performance of the members of its staff. These security controls are documented in a policy and include the areas below.

5.3.1 Qualifications, Experience, and Clearance Requirements

AB Svenska Pass performs checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks include:

- Criminal convictions for serious crimes;

- Misrepresentations by the candidate;
- Appropriateness of references;
- Any other clearances, as deemed appropriate.

5.3.2 Background Check Procedures

Recruitment of the right personnel is crucial for the security of the production facility and this is performed by the HR department. Before a person is employed, both their background (register checks, financial checks, references etc.,) and skills sets are investigated. All data in this security screening, including the decision to offer employment are saved in the person's file. Decisions on employment are taken by the HR manager, employing manager and security manager.

The security related responsibilities of each employee are defined and described in their work duties descriptions. When a person is allocated a sensitive task or position of trust, a check is also made on conflicts of interest and that an adequate division of work duties has been assured.

Background checks are run on all employees, irrespective of role or department and security screened (SUA) annually.

5.3.3 Training Requirements

Every employee at Thales DIS Sweden and AB Svenska Pass is always given the same basic training on security and quality. This training includes information on our general security and quality principles and instructions. In addition to this basic training, persons that work in different departments and in different roles are offered the opportunity of specific and dedicated training within security and quality.

All employees must take a basic course in security and quality at least once a year. Security and quality information is also distributed as necessary on the intranet, by email and in group meetings.

5.3.4 Retraining Frequency and Requirements

Periodic training updates might also be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job Rotation Frequency and Sequence

Not stipulated.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of ABSP PKI policies and procedures. Disciplinary actions may include measures up to and including termination of employment and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements

Any contractor commissioned must also be SUA approved at the respective employer and sign a security protection agreement with the respective authority. With the exception of customer visits, there is a general ban on visitors at AB Svenska Pass production sites.

5.3.8 Documentation Supplied to Personnel

AB Svenska Pass makes documentation available to personnel, during initial training, retraining, and during other occasions.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. The CA implements the following controls:

The CA event logging system records events that include but are not limited to:

- Registration information
- generation of a certificate;
- Revocation of a certificate;
- Publishing of a CRL.

AB Svenska Pass audits all event-logging records. Audit trail records contain:

- The identification of the operation;
- The date and time of the operation;
- The identification of the certificate involved in the operation;
- The identity of the transaction requestor.

In addition, AB Svenska Pass maintains internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

- Start and stop of servers; Outages and major problems;
- Physical access of personnel and other persons to sensitive parts of the AB Svenska Pass site;
- Back-up and restore;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.
- All incidents in the security system
- CCTV - Recorded material from surveillance cameras

AB Svenska Pass ensures that designated personnel review log files at regular intervals and detects and reports anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of the CA, the RA and designated auditors. The log files shall be properly protected by an access control mechanism. Log files and audit trails are backed up.

5.4.2 Frequency of Processing Log

The Auditor reviews the audit logs in search of anomalies or alerts on a regular basis.

5.4.3 Retention Period for Audit Log

Documents are stored for at least 10 years unless the Data Protection Act or other legislation requires removal. The authority has specified a requirement concerning the preservation of documents and order file that are received from the authority in the security protection agreement the procuring authority has with AB Svenska Pass. In a corresponding way, the authority has a contractual liability to AB Svenska Pass to preserve all documents in accordance with the rules and regulations that apply to an issuer of Swedish eID.

Other documentation is stored physically at AB Svenska Pass for at least 10 years in accordance with internal processes for document preservation.

5.4.4 Protection of Audit Log

Only trusted members of staff, that are assigned the Auditor role, may access the AB Svenska Pass archive. Measures are taken to ensure:

- Protection against modification of archive, such as storing the data on a write once medium;
- Protection against deletion of archive;
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media.

5.4.5 Audit Log Backup Procedures

A differential back up of AB Svenska Pass archives is carried out on a daily basis, during working days.

5.4.6 Audit Collection System.

AB Svenska Pass archive collection system is internal.

5.4.7 Notification to Event-Causing Subject

Not applicable.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Security vulnerability assessments are performed, reviewed, and revised. These assessments are based on real-time automated logging data and are performed on a regular basis.

5.5 Records Archival

5.5.1 Types of records archived

AB Svenska Pass keeps internal records of the following items:

- All certificates for a period of a minimum of 10 years after the expiration of each certificate;
- Agreements, policy documents and practice statements,
- Audit trails on the issuance of certificates for a period of a minimum of 10 years after expiration of a certificate;
- Audit trail of the revocation of a certificate for a period of a minimum of 10 years after revocation of a certificate;
- CRLs for a minimum of 10 years after publishing;
- AB Svenska Pass should retain the very last back up of the CA archive for 10 years following the issuance of the last certificate.

5.5.2 Retention period for archive

Retention periods are defined in 5.5.1

5.5.3 Protection of archive

AB Svenska Pass keeps archives in a retrievable format. AB Svenska Pass ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

AB Svenska Pass retains in a trustworthy manner records of digital certificates, audit data, AB Svenska Pass systems information and documentation and records of digital certificates for a term as indicated above.

Only the AB Svenska Pass member of staff assigned to records retention duty may access the archive. Measures are taken to ensure:

- Protection against modification of archive, such as storing the data on a write once medium;
- Protection against deletion of archive;
- Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media.

5.5.4 Archive Backup Procedures

A back up of AB Svenska Pass archives is carried out.

5.5.5 Requirements for Time-Stamping of Records

All iCA components are synchronized with a time service; a Network Time Protocol (NTP) Service. Time derived from the time service shall be used to establish the time of:

- Initial validity time of a CA Certificate
- Revocation of a CA Certificate
- Posting of CRL updates

5.5.6 Archive Collection System (Internal or External)

The TSP archive collection system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized personnel in Trusted Roles are allowed access to the archive.
Should records concerning the operation of services be required to provide evidence of the correct operation of the services or for the purpose of legal proceedings, they

are made available to legal authorities and/or persons whose right of access to them arises from the law.
The integrity of the information is verified during recovery tests. The archive systems with built-in integrity controls are in use.

5.6 Key Changeover

A subscriber private key cannot be renewed but requires a new application for an ID Card and corresponding eID.

A renewal of a CA key will follow a key changeover process, where the new key will be created before the end of the existing key´s lifetime for creating new certificates.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

To ensure the effective and rapid management of security incidents, Thales has defined a global procedure for incident management, which is one of the main procedures at all Thales production facilities.
All such measures are implemented based on ISO 27001.
The security manager is the contact person for the procuring authority and they are to be notified without delay.
All deviations must be investigated to identify the root cause, they must be managed quickly and in accordance with the classification and the effectiveness of the corrective measures must be checked/evaluated.

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

AB Svenska Pass establishes the necessary measures to ensure full and automatic recovery of the service in case of a disaster, corrupted servers, software or data.

5.7.3 Entity private key compromise procedures

In case of a suspected or known compromise of a private key, the ABSP Crisis procedures shall be enacted with approval from ABSP-TSEB. Notification to involved parties is performed through a communication plan and in the case CA Certificate revocation is required, the revoked status is communicated to relying parties through the CRL which is published on the AB Svenska Pass eID website.

5.7.4 Business continuity capabilities after a disaster

AB Svenska Pass has the capability to recover its CA operations following a disaster with support for all the key functions i.e. certificate issuance, certificate revocation, and publication of CRL information. Thales has a structured method for crisis management that is used at all sites worldwide. The method is described in a document called Thales DIS Crisis Management Framework.

Each site has its own crisis management team. The first step is for the Thales management to appoint a Crisis Management Leader per site worldwide. These are

then sent on a one-week training course on the structured crisis management method chosen by Thales.

The local crisis management leader then selects a local crisis management team and allocates specific roles to each team member. The roles are described in the Thales Crisis Management Framework document.

One such role is Incident Assessment Coordinator (IAC) who is tasked with being sent the alarm by email or phone from employees or other stakeholders that we have a crisis situation. IAC then makes an assessment whether to summon the local crisis management team and/or if it is so serious that the central crisis management team in Paris should be contacted.

Crisis Management Team Älvsjö has regular and minuted meetings designed to ensure the team is well-prepared in the event of a crisis arising. The first thing we have done is to identify what crises are the most likely to occur at our site in Älvsjö. Based on these, we have developed an action plan per potential crisis. The aim is to be as well-prepared as possible if a crisis arises and to ensure we get back to normal operations/production as soon as possible.

5.7.5 CA or RA termination

In the case that a CA in this CP/CPS must be taken out of operation, AB Svenska Pass will take all reasonable steps to make this information public as soon as possible and where possible, notify individual parties including subscribers, relying parties and other directly affected entities. For planned actions, termination plans will be set up in advance.

The termination of CA operations is to be viewed as the situation when all service associated with the CA is ended, i.e. not the same as the CA changing root certificate.

Before CA ends its operations, all trusted parties and customers will be notified.

Delete the CA's private key.

Block service and check service cease

Repository is saved for traceability, this includes policy, issuer declaration.

In the case that an RA ceases to be a part of the AB Svenska Pass PKI, a back-up routine for the revocation process will be performed by the former RA or AB Svenska Pass will revoke all e-IDs connected to that RA.

6 Technical Security Controls

6.1 Key pair generation and installation

ABSP PKI uses a trustworthy process for the generation of its CA private keys according to a documented procedure. All key ceremonies for generating keys are based on multi person control and occupied by roles in the CA organization. In addition to passwords and personal log in of PED key bearers with duality, key ceremonies also require the presence of at least one additional witness. These ceremonies are documented and signed by all persons present.

6.1.1 Key pair generation

Root CA and subordinate CA key pairs have been generated in an HSM that meets at least FIPS 140-2 level 3 and EAL4+ requirements. Access to the HSM within the CA environment is restricted by the use of smartcard. The HSM is always stored in a physically secure environment and subject to security controls throughout its lifecycle.

The subscriber private key is generated by the RA on and by the QSCD or in a secure environment and injected into the QSCD. Once in the QSCD, the private key cannot be extracted.

Before the subscriber key generation and initialization:
Non-initialized QSCD cards shall be controlled and registered at the delivery from the hardware manufacturer and are kept in a secured way with the delivery batches intact. Access to the secured location, containing the non-initialized cards and devices is restricted in such a way that two-persons need to be present at all times.

The Generation of private keys and personalization of QSCD equipped cards are done in batches which are processed in the order they have been initialized. Every step in the process is documented both electronically and on a printed report that follows the batch through all production steps.

After **subscriber key generation and initialization:**
Initialized but not personalized batches of QSCD equipped cards and remaining cards from partly used batches, are kept in the same secured manner as the non-initialized cards and devices and managed under dual control.

After the subscriber card personalization:
Personalized QSCD equipped cards are always kept separated from non-personalized cards. Descriptions regarding possible discrepancies in production failures, failures in the delivery processes and in the event of lost or defective cards will be logged and subject to documentation.

6.1.2 Private key delivery to subscriber

QSCD equipped cards are distributed via the ID Card issuer.

AB Svenska Pass eID is supplied on a contact chip on a card, plus antenna (both contact and contactless interface). The chips are evaluated and certified according to a series of common criteria, such as IASv4.4 at MultiAppv4.0.1 that is certified to

EAL5+ for PP-QSCD.

The chips also contains both hardware and software based measures against various types of attack, side channel attacks, invasive attacks and DFA and advanced fault attacks.

The chips are coded such that after a number of incorrect PIN code attempts, a PUK code is required. The number of attempts with a PUK code is also limited. If this is exceeded, the eID becomes invalid and a new eID must be applied for.

The QSCD equipped cards are only handed out to the subscriber personally according to the routines for the ID Card issuer.

Receipt of the QSCD equipped card is signed by the subscriber. The signed receipt is kept for at least ten years.

The provision of eID is done via a visit in person to the authority, where the applicant must identify him/herself. Activation data in the form of a PUK code is sent to the applicant's registered address.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber public key is transferred from the ID Card issuer after key pair generation to the CA by means of encrypted message over a secured connection.

6.1.4 CA Public Key Delivery to Relying Parties

All relying parties who want to use ABSP CA public keys should download them from:

- ABSP website :
  - http://va.absvenskapass.se/absvenskapass-class1-iCA-v1-2.crt
  - http://va.absvenskapass.se/absvenskapass-class1-rootCA-v1.crt

6.1.5 Key sizes

ABSP Root CA keys are generated as ECC keys with a length of 384 bits.
ABSP Issuing CA keys are generated as ECC keys with a length of 256 bits.
The subscribers' keys are generated as ECC keys with a length of 256 bits.

6.1.6 Public key parameters generation and quality checking

All CA keys are generated by HSMs conformant to FIPS 140-2 level 3,
Subscribers' keys are generated either in in QSCD cards or in a secure environment.

The secure chip module of the card is certified to Common Criteria Level EAL5+ Secure Signature Protection Profiles PP-BSI-0059-QSCD-P2 and BSI-PP-0075-QSCD-P3

6.1.7 Key usage purposes

The key usage flags are populated in Root CA, Issuing CA and subscriber certificates.

ABSP PKI ensures that the use of Root CA and Issuing CA private keys is strictly controlled, as indicated by the flags, i.e. only for certificate and CRL signing. Subscribers should use their private keys only for the purposes indicated in the respective certificates.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

Root and Issuing CAs keys are generated in an HSM meeting FIPS 140-2 level 3 and EAL4+ requirements.
The subscriber's private keys are created and stored in the chip of the QSCD equipped card. The keys will be generated and protected in a cryptographic module certified as Common Criteria EAL 5+. The protection profile, such as information structure and information access rights, of such QSCD needs to be approved by AB Svenska Pass before the device is allowed to carry AB Svenska Pass e-ID.

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

Controls are implemented to ensure that multiple trusted personal are required in order to access Root and iCA private keys

6.2.3 Private key escrow

ABSP PKI CA keys are not in escrow. Subscriber keys used for authentication and signature purposes are not in escrow.

6.2.4 Private key backup

ABSP Root CA and iCA private keys are backed up in HSMs located off site, for disaster recovery purposes. ABSP PKI does not store copies of subscriber private keys.

6.2.5 Private key archival

ABSP PKI does not archive private keys of its issued certificates.

6.2.6 Private key transfer into or from a cryptographic module

Root CA and subordinate CA private keys are cloned from the master HSM to the backup HSM.
Private keys used for authentication or signing cannot be copied from the QSCD card.

6.2.7 Private key storage on cryptographic module

ABSP PKI keys are stored in hardware cryptographic modules and can only be used after key activation.

6.2.8 Method of activating private key

Root CA and subordinate CA private keys are activated with the presence of at least 2 trusted ABSP PKI personal each possessing a token and corresponding PIN.
In the AB Svenska Pass e-ID, a card holder must be authenticated to the QSCD before the activation of the private keys. This authentication is done using a PUK as activation data for all private keys.

6.2.9 Method of deactivating private key

The Root CA keys are deactivated by logging out of the HSM, terminating the session with the HSM, removing the CA token from the computer or by powering down the system.

Subscribers are responsible for the deactivation of their own private keys.

6.2.10 Method of destroying private key

Keys will be destroyed by ABSP PKI trusted roles when they are no longer required. Destruction is done when the key is no longer usable, based on 3 criteria:

Not needed for card production. Not needed for recall of key generated earlier. Not needed from an evidence perspective, or for data recovery for future investigations.

Software keys are destroyed by overwriting the key material. Deletion of individual keys held in HSMs is performed by the HSM, which ensures that they cannot be used. The HSM shall be zeroised when none of the keys that it contains are required. This HSM function destroys all keys without requiring that the hardware be physically destroyed.

Destruction means the destruction of all key copies, backup and archiving. Destruction is irreversible. All destruction of sensitive material or equipment must be done under duality control, documented and signed by everyone present. The key values must not be visible during destruction.

6.2.11 Cryptographic Module Rating

Refer to the clause 6.2.1 of this CP/CPS

6.3 Other aspects of key pair management

6.3.1 Public Key Archival

All public keys, such as Root CA's, issuing CAs' and subscribers' that are used for verification purposes are archived, as integral parts of the certificates issued, for at least ten years (for details on archival see 5.5).

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

ABSP PKI certificates validity periods are:
− 20 years for ABSP Root CA.
− 10 years for the issuing CAs.
− A maximum of 5 years for subscriber certificates.

The usage periods for the private signature keys are:
− 10 years for ABSP Root CA.
− 5 years for the issuing CAs.
− A maximum of 5 years for subscriber certificates.

6.4 Activation data

6.4.1 Activation data generation and installation

ABSP Root CA and Issuing CA keys are activated according to the specifications of the hardware manufacturer and documented AB Svenska Pass Processes.
All subscribers' private keys are protected by PINs of at least six digits and a PUK of eight digits.

To be able to use the certificate, activation is required. This is done with the aid of an activation code that is sent to the holder's registered address.
The subscribers' PUK codes are stored encrypted at the card manufacturer appointed by AB Svenska Pass, and can, if agreed in applicable agreements, be distributed to the subscriber's home address by registered mail after a separate request from the subscriber.

6.4.2 Activation data Protection

ABSP Root CA and Issuing CA activation data is distributed over multiple physical keys. The activation data required to use the private keys on the QSCD is communicated to the subscriber by RA administrator or sent to the subscriber's home address according to the Swedish SPAR register or equivalent register approved by AB Svenska Pass.

The activation code is processed separately to the production of cards. The authority does not have access to the activation code. When the holder has activated their eID, they are asked to choose a PIN code for the certificate.

AB Svenska Pass e-ID may not be used by any other person than the subscriber. If the subscriber suspects that another person may have knowledge of the activation data, the subscriber shall, as said in the agreement, immediately change the activation data or make a revocation request for the ID Card*. The requirements on how this PIN is to be protected is stated in the Terms and Conditions for eID, and when taking receipt of the eID.*

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

The CA implements appropriate computer security controls including physical and logical access controls, role separation, multi-layered controls, intrusion detection, and multi-factor authentication processes for all personnel who can cause the issuance of a certificate or cause a person to become able to issue a certificate.

6.5.1 Specific computer security technical requirements

The CA provides the following functionality through the operating system and a combination of the operating system, the PKI software and physical controls:

- access control to CA services and PKI roles;
- enforced separation of duties for PKI roles;
- identification and authentication of PKI roles and associated identities,
- use of cryptography for session communication and database security;
- archival of CA and end entity history and audit data;
- audit of security related events;
- recovery mechanisms for keys and the CA system.

Information on this functionality is provided in the respective sections of this CP/CPS.

6.5.2 Computer security rating

Not applicable

6.6 Life cycle technical controls

6.6.1 System development controls

All hardware and software procured for operating an Issuing CA shall be purchased in a manner that will mitigate the risk that any particular component could be tampered with. Equipment developed for use within the eID PKI shall be developed in a controlled environment under strict change control procedures.
A continuous chain of accountability, from the location where all hardware and software that has been identified as supporting an Issuing CA within the eID PKI, must be maintained by ensuring that it is shipped or delivered via controlled methods. Issuing CA equipment shall not have any application or component software installed on it that is not part of the Issuing CA configuration.

6.6.2 Security management controls

All subsequent updates to Issuing CA equipment must be purchased or developed in the same manner as the original equipment and be installed by trusted and trained personnel in a defined manner.

The system application for the CA is not internally developed. The system application has a common criteria certificate, EAL4+.

All operating systems are hardened, patching and modifications are made after risk evaluation and in accordance with the change process. All systems are redundant and changes are tested in test and staging environments first. Support agreements with suppliers of software and hardware are in place and continuously secured.

Architecture and processes are developed in accordance with industry best practice and audited regularly internally and by certified auditors for each respective certification standard.

6.6.3 Life Cycle Security Controls

The CA employs a configuration management methodology for the installation and ongoing maintenance of the Certificate Authority systems. The Certificate Authority software, when first loaded will provide a method for the CA to verify that the software on the system originates from the software developer and has not been modified prior to installation.

All changes are tested and verified in test and commissioning environments in accordance with change management and risk management plans. Production systems are redundant which enables stepless production commissioning and secure fall back.

6.7 Network security controls

The CA maintains a high-level network of systems security including firewalls. Network intrusions are monitored and detected. Specifically:

- All communications between the CA and the RA operator regarding any phase of the life cycle of Citizen Certificates are secured with PKI based encryption and signing techniques, to ensure confidentiality and mutual authentication. This includes communications regarding certificate requests, issuance, and revocation.
- The CA web site provides for encrypted connections through the Secure Socket Layer (SSL) protocol.
- The CA network is protected by a managed firewall and intrusion detection system.
- It is prohibited to access sensitive CA resources including CA databases from outside of the CA operator's own network.
- Internet sessions for request and delivery of information are encrypted.
- Logical separation is done via several logically separated networks. DMZ for validation of certificates protected by an external firewall cluster, behind which is an IDS (intrusion detection system) from another developer, behind this is gWAF (Thales Application Firewall) before a load balancer divides the traffic to the OCSPs.
- Dedicated network for administration of CA systems and the PKI operational network are separated. Systems used for administration of the security policy implementation are not used for other purposes. Also the production systems for the CA services are separated from systems used in development and testing.

6.8 Time-stamping

All log entries are individually time stamped. The time is taken from the Swedish Distributed Time Service following UTC (SP). Time derived from the time service shall be used to establish the time of:

- Initial validity time of a CA Certificate
- Revocation of a CA Certificate

- Posting of CRL updates

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate profile

The certificate profile defines the fields that shall be present in a certificate. The certificate profile of the certificates in ABSP PKI follows the version 3 profile defined in the ITU X.509 standard. The profile of the certificates also follows the document RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [6].

The basic fields used in certificates are listed in the table below:

Certificate field	Description
Version	This field states which of the certificate versions defined in the X.509 standard the certificate conforms to. The issued certificates conform to the version 3.
Serial number	The CA generates a unique serial number for each certificate. The software manages the uniqueness of the serial number automatically.
Signature algorithm	The signature algorithm is the set of mathematical rules according to which the CA software executes the signing of the certificate. Identifiers have been allocated for the algorithms that are generally used. The identifier of the algorithm used for the signing of the certificate is given in this field. The signature cannot be verified if the algorithm used is not known. The hash algorithm used is sha256 or sha384.
Issuer	This field states the name of the Issuer of the certificate.
Not Before	This field states the date after which the certificate is valid.
Not After	This field states the date after which the certificate is no more valid.
Subject	This field identifies the CA name under whose possession the private key is, that corresponds to the public key contained in the certificate. The field includes the unambiguous name of the Subject.
Key Specification	This field states the type of keys that are used. The key type used is ECC: secp 256r1 (iCA) and secp384r1 (RCA)

7.1.1 Version number

All issued certificates are X.509 Version 3 certificates, in accordance with RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

7.1.2 Certificate extensions

Certificate extensions will be used in accordance with RFC 5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”. The extensions are mandatory except for Authority Key Identifier which is optional in self-signed CA certificates.

The certificate extensions are described in AB Svenska Pass eID Naming and Profile.

7.1.3 Cryptographic algorithm object identifiers

Root CA Signature algorithm: ecdsa-with-SHA384 *1.2.840.10045.4.3.3*
Sub CA Signature algorithm: ecdsa-with-SHA256 *1.2.840.10045.4.3.2*

7.1.4 Name forms

Each DN will be in the form of an X.501 Directory String.

7.1.5 Name constrains

Subject and Issuer DNs comply with PKIX standards and are present in all certificates. The name fields used are Issuer Distinguished Name and Subject Distinguished Name.

All attributes are mandatory.

All attributes are described in the document AB Svenska Pass eID Naming and Profile Document.

7.1.6 Applicable CP OID

The certificate policy object identifier will be present in issued certificates and will contain the OID of this CP/CPS according to section 1.2.

7.1.7 Usage of the policy constrains extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifier CPS uri is used in the subscriber certificates. The value of the CPS uri points to AB Svenska Pass CA Repository (https://va.absvenskapass.se/CPS2) where this CP/CPS is published.

7.1.9 Processing semantics for the critical CP extension

Not applicable.

7.2 CRL profile

The CRL profile is described in the document AB Svenska Pass eID Naming and Profile Document.

7.2.1 Version number

Certificate status control is only available via the OCSP responders.

7.2.2 CRL and CRL entry extensions

The CRL and CRL entry extensions are described in the document AB Svenska Pass eID Naming and Profile Document.

7.3 OCSP profile

The OCSP profile is described in the document AB Svenska Pass eID Naming and Profile Document.

7.3.1 Version number

Version 1 of the OCSP specification as defined by RFC2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol “is implemented for the OCSP responders.

7.3.2 OCSP extensions

The OCSP Nonce extension should be used in OCSP requests.

8 Compliance audit and other assessments

The AB Svenska Pass PKI conducts periodic audits indicating the Root CA and its subordinate CAs compliance with the trust framework for the Swedish eID [2]-level 4.

8.1 Frequency or circumstances of assessment

A compliance audit is performed by the eID board each 3 years,
Over of a 3-year period the CA shall be subject to internal audit, conducted by an internal independent control function, unless the size of the organization or other viable reason justifies the audit to be conducted in another manner.

Further the CA is annually audited to be compliant to ISO 27001.

8.2 Identity/qualifications of assessor

The audit services shall be performed by an organizational independent, recognized, credible, and established auditor, experienced in performing information security audits, having significant experience with PKI and cryptographic technologies.

8.3 Assessor's relationship to assessed entity

The auditor and the Root and Issuing CA under audit must not have any relationship that would impair the auditor’s objectivity.

8.4 Topics covered by assessment

The purpose of the compliance audit is to verify that all routines and processes used for issuing AB Svenska Pass e-ID complies to the Swedish Trust Framework – level 4 requirements by e-ID board.

8.5 Communication and actions taken as a result of deficiency

If anomalies are discovered, they will be reported to the AB Svenska Pass TS Executive Board. The ABSP-TSEB is responsible for acting upon the compliance audit written report.

8.6 Communication of Results

The audit report will be communicated internally and is not available on Internet for relying parties.

9 Other Business and Legal Matters

9.1 Fees

Fees for ABSP CA Service are defined in applicable customer agreements, or if applicable the e-ID board agreement (“Valfrihetssystem 2017 E-legitimering”)

9.2 Financial responsibility

AB Svenska Pass will maintain adequate levels of financial resources to support its business practices.

9.2.1 Insurance coverage

AB Svenska Pass maintains reasonable levels of insurance coverage.

9.2.2 Other assets

AB Svenska Pass shall maintain sufficient assets and financial resources to fulfil its responsibilities according to this CP/CPS.

9.2.3 Insurance or warranty coverage for end-entities

The issuing of AB Svenska Pass e-ID in accordance to this CP/CPS does not mean AB Svenska Pass shall be seen as an agent, fiduciary or other representative of a subscriber or relying party. Subscribers or relying parties have no authority to bind AB Svenska Pass by agreements or by any other means, to any obligation.

Relying parties must apply to commercial insurance providers for their own protection against financial loss.

9.3 Confidentiality of business information

9.3.1 Scope of considered confidential information

Personal or corporate information held by AB Svenska Pass related to the issuance of AB Svenska Pass e-ID, is considered confidential and will not be released without the prior consent of the relevant party unless it is excluded in section 9.3.2 or otherwise defined as public in this CP/CPS or by law.

9.3.2 Information considered outside the scope of confidential information

The following information is not deemed to be confidential:
a) Issued certificates including public keys.
b) OCSP responses.
c) Subscriber terms and conditions.
d) This CP/CPS.

Exceptions may apply to subscriber information if this is stated in a specific agreement between AB Svenska Pass and the subscriber’s employer or any other organization from which the subscriber has received a QSCD equipped ID Card with containing an AB Svenska Pass e-ID. In case the RA is a Swedish government some otherwise confidential information, i.e. information regarding the subscriber’s application and

reception of AB Svenska Pass e-ID, may be regarded “public” according to the Swedish law.

9.3.3 Responsibilities of participants to protect confidential information

All confidential information will be physically and/or logically protected from unauthorized reading, modification or deletion. Storage media used by the CA systems are protected from environmental threats such as temperature, humidity and magnetism and this also applies to backup and archive media.

AB Svenska Pass will disclose confidential information if a court of law or any other legal authority subject to Swedish law so decides. Private keys in QSCD are not stored by AB Svenska Pass or any of its subcontractors and can for that reason never be disclosed.

9.4 Privacy of personal information

Where appropriate, personal data will be saved at the authority that stores all personal data according to the Data Protection Act. ABSP’s personalisation facility for ID documents accepts orders for eID containing personal data such as name, date of birth, civil registration number and signature, these are saved in accordance with the Data Protection Act. Names and civil registration numbers are sent to ABSP CA. This information is saved together with the card number that the certificate will be placed on. The information is saved to be able to authenticate and validate the eID. ABSP is the data protection officer on behalf of the authority that provided the personal data.

9.4.1 Privacy plan

AB Svenska Pass will not disclose any personal information as long as the information is not considered public and unless it is required by law. In general all information not stated in 9.4.3 is treated as private and will not be disclosed by AB Svenska Pass without the consent of the subscriber.

9.4.2 Information considered private

Any information about subscribers and requesters that is not made public through the certificates issued by this CA and the CRL is considered private information.

9.4.3 Information not considered private

Publicly available information such as, issued certificates including subscriber information and public keys and OCSP revocation information is not considered to be private information where certificates are used or managed.

9.4.4 Responsibility to protect private information

See section 9.3.3.

9.4.5 Notice and consent to use private information

Subscribers have agreed to allow their personal information to be submitted in the registration process.

9.5 Intellectual property rights

All ABSP intellectual property rights including all trademarks and copyrights of all ABSP's documents remain the sole property of the ABSP.
In accordance with the Swedish Copyright Act, no part of this CP/CPS may be reproduced, published or transmitted in any form without written permission from AB Svenska Pass.

9.6 Representations and warranties

9.6.1 CA representations and warranties

AB Svenska Pass shall operate in accordance with this CP/CPS, when issuing and managing AB Svenska Pass e-ID and will ensure that the RAs operating on its behalf comply with the relevant provisions of this CP/CPS. AB Svenska Pass will take commercially reasonable measures to ensure that subscribers and relying parties are aware of their respective rights and obligations with respect to the operation and management of any keys, certificates or end-entity hardware and software used in connection with AB Svenska Pass e-ID.

AB Svenska Pass warrants that the information in the AB Svenska Pass´ e-IDs issued by AB Svenska Pass is checked and verified in accordance with the routines that have been stated in this CP/CPS. AB Svenska Pass liability is limited to its contractual agreements with the subscriber.

9.6.2 RA representations and warranties

AB Svenska Pass requires that all RAs comply with the relevant provisions of this CP/CPS. The RA is responsible for keeping the internal administrative routines that individual responsibility for the identification and authentication of subscribers following section 3.1 and section 4.1.can be proved.

9.6.3 Subscriber representations and warranties

AB Svenska Pass requires that all subscribers of AB Svenska Pass e-ID comply with the relevant provisions of this CP/CPS. The subscriber is bound through an agreement with AB Svenska Pass and will need to accept the subscriber application form before receiving AB Svenska Pass e-ID. Subscribers are required to protect their QSCD equipped ID Card and associated activation data (PIN/PUK) in accordance with the subscriber agreement, and to take all reasonable measures to prevent their loss, disclosure, or unauthorized use. The subscriber shall also ensure that the activation data (PIN/PUK) has not been shared with any other person, and the letter is intact and unopened upon receipt. The subscriber shall only use the keys and certificates for the purposes identified in this CP/CPS and in the subscriber agreement. When a subscriber suspects a private key compromise, the subscriber shall immediately call AB Svenska Pass revocation service to ensure the e-ID is revoked.

9.6.4 Relying party representations and warranties

AB Svenska Pass requires that relying parties comply with all the relevant provisions of this CP/CPS. Prior to accepting an AB Svenska Pass e-ID, a relying party is responsible for:

- Verifying that the certificate is appropriate for the intended use.

- Checking the validity of the certificate, i.e. verify the validity dates and the validity of the certificate and issuance signatures.
- Checking the status of the certificate against the appropriate OCSP responder in accordance with the requirements stated in this CP/CPS. As part of this verification process the digital signature of the OCSP responder should also be validated. If certificate status can't be received due to system failure or similar, the certificates shall not be accepted.
- End entity certificate chain should be uploaded from ABSP website as defined in 2.1.

It is also up to the relying party to study this CP/CPS to determine whether the liability limitation of the certificate is appropriate for the actual application where it is to be used. AB Svenska Pass will provide certificate status information identifying the access point to the OCSP responder in every certificate AB Svenska Pass issues in accordance with section 4.9.6 and 4.9.9.

9.7 Disclaimers of warranties

AB Svenska Pass warrants that the information in the AB Svenska Pass e-ID is checked and verified in accordance with the routines that have been stated in this CP/CPS. In the case AB Svenska Pass uses a subcontractor to perform parts of the service, AB Svenska Pass is responsible as if AB Svenska Pass itself had performed the tasks.

9.8 Limitations of liability

AB Svenska Pass' liability is limited to what is stated in the, at each time, valid terms and conditions for AB Svenska Pass e-ID.

9.9 Indemnities

The subscriber agreement regulates all questions regarding indemnities. The applicant accepts the subscriber agreement at the same time as he or she applies for the AB Svenska Pass e-ID and is bound by the terms and conditions when receiving the AB Svenska Pass e-ID.

9.10 Term and termination

9.10.1 Term

This CP/CPS becomes effective after publication in the ABSP PKI repository. Amendments to this CP/CPS become effective after publication in the ABSP PKI repository.

9.10.2 Termination

This CP/CPS remains in force until it is amended or replaced by a new version.

9.10.3 Consequences of termination of the document

The conditions and effect resulting from termination of this document will be published on ABSP CA repository https://va.absvenskapass.se/repository

9.11 Individual notices and communications with participants

The appropriate provisions to handle notices are defined in applicable agreements with the relevant participants.

9.12 Amendments

ABSP-TSEB is responsible for reviewing and approving changes to this CP/CPS.

9.12.1 Procedure for amendment

CP/CPS publication will be done in accordance with section 2.
An electronic copy of this CP/CPS is to be made available via https://va.absvenskapass.se/CPS2.

9.12.2 Notification mechanism and period

- Minor changes that do not affect the security levels in processes and regulations described can be made without notice.
- Changes to contact details can be notified at time of change.
- Changes that affect processes and regulations must always be notified to PKI participants defined in 1.3 at least 30 days in advance.

The ABSP-TSEB may provide notice, in writing, of any proposed changes to this CP/CPS, if the judgement and discretions of ABSP-TSEB the changes may have significant impact on the issued certificates or AB Svenska Pass TS services.

9.12.3 Circumstances under which OID requires to be changed

If a CP/CPS change is determined by ABSP-TSEB to warrant the issuance of a new CP/CPS, ABSP-TSEB will assign a new object Identifier (OID) for the new CP/CPS.

9.13 Dispute resolution provisions

If a dispute relating to this CP/CPS is not successfully resolved through negotiations the dispute will be resolved according to Swedish law and Swedish court.

9.14 Governing law

Swedish law shall apply to the interpretation of this CP/CPS, if not otherwise agreed.

9.15 Compliance with applicable law

This CP/CPS is subject to applicable law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

AB Svenska Pass shall not be held responsible for any delay or failure in provision of its obligations that results from events beyond its control such as acts of God, acts of terrorism and war, fire, flood, strike, power or telecommunication services failure or other similar causes beyond its reasonable control and without the fault or negligence of AB Svenska Pass or its subcontractors.

9.17 Other provisions

No stipulation.

10 Appendix A

10.1 Definitions and acronyms

Term	Abbreviation	Explanation
Advanced electronic signature	AES	An electronic signature which meets the following requirements: a) It is uniquely linked to the signatory; b) it is capable of identifying the signatory; c) it is created using means that the signatory can maintain under his sole control; and it is linked to the data to which it relates in such manner that any subsequent change of the data is detectable (see Directive 1999/93 EC)
Attribute		Information bound to an entity that specifies a characteristic of an entity, such as a group membership or a role, or other information associated with that entity.
Certificate		Public key of a user together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it. The certificate format is in accordance with ITU-T Recommendation X.509.
Certification authority	CA	Authority trusted by one or more users to create and assign certificates.
CA certificate		Certificate which certifies that a particular public key is the public key for a specific CA.
Certificate's certificate chain		
Certificate level		Certificates can exist at two levels: primary certificates and secondary certificates.
Certificate policy	CP	Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification practice statement	CPS	Statement of the practices which a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
Certificate revocation		The process of removing a certificate from the management system and indicating that the key pair related to that certificate should no longer be used.
Certificate revocation list	CRL	Signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.
Certificate request syntax	CRS	
Certification services provider	CSP	Entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
Digital signature		The result of the transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine that the key that corresponds to the

		signer's key created the transformation and the message was not altered. As defined in the ITU-T Recommendation X.509.
Directive 1999/93/EC		The European Directive on Electronic Signature, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999.
Distinguished name	DN	The unique identifier for the holder of a certificate
	ETSI	European Telecommunications Standards Institute
E-ID		A Swedish name of the TeleTrusT Token. The translation was made by the Swedish Post when starting its production in 1994 of physical ID cards equipped with a chip that met the security and administrative requirements set in the TeleTrusT concept. Since then a Swedish e-ID has two key pairs with at least two certificates, one "digital signature certificate" for electronic signatures and one "confidentiality certificate" to be used for authentication and/or encryption services. See ITU-T Recommendation X.509.
Electronic signature		Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication of that data. The term was introduced by TeleTrust 1987. It is technically equivalent to digital signature but as a part of the TeleTrusT concept, also human acceptance and legal needs must be taken into consideration. For that reason the term electronic signatures became since then the term used in legal contexts. See TeleTrusT Token and the Directive 1999/93/EC.
	FIPS	Federal Information Processing Standard
	IETF	Internet Engineering Task Force
	IP	Internet Protocol
	ISO	International Organization for Standardization
	ITU	International Telecommunications Union
	LDAP	Lightweight Directory Access Protocol
	NIST	National Institute of Standards and Technology
Object identifier	OID	The unique identifier registered under the ISO registration standard to reference a specific object or object class.
Key		A unique, generated electronic string of bits used for encrypting, decrypting, e-signing or validating digital signatures.
Key holder		In this document a natural person that has exclusive control of the private key where the public equivalent is certified in a certificate. See subscriber.
Key pair		Two related keys, one being a private key and the other a public key having the ability whereby one of the pair will decrypt the other.
Private key		A key forming part of a key pair that is required to be kept secret and known only to the person that holds it.
Public key		A key forming part of a key pair that can be made public.
Relying party		Recipient of a certificate which acts in reliance on and/or digital signatures verified using that certificate.
	URI	Universal Resource Indicator - an address on the Internet.

Non-repudiation		Protection against the denial of the transaction or service or activity occurrence.
Non-repudiation services		Service which aim to hold a key holder responsible for signed messages or document and verified by a third party at a later time.
Trusted third party	TTP	A party on which two or more collaborative parties rely. A TTP carries out services for the collaborative parties, such as time-stamping, certificate issuing, etc.
Root certification authority certificate		Self-signed certificate issued to the root certification authority.
Online certificate status protocol	OCSP	
Personal identification number	PIN	A number code that enables the card holder to use services associated with private key linked to that certificate.
Personal unblocking key	PUK	When a PIN is blocked through three consecutive incorrect PIN verifications, the PIN may only be unblocked through a special unblocking procedure, defined in the issuer's policy declaration.
Personnummer		The personnummer is the national identity number that consists of a natural person's date of birth followed by three digits and one check digit (YYYYMMDDNNNC).
Public key infrastructure	PKI	A system for publishing the public key values used in public key cryptography. Also a system used in verifying, enrolling, and certifying users of a security application.
Registration authority	RA	Here an entity designated by AB Svenska Pass to operate within its PKI responsible for identification and authentication of card holders.
	SFS	Svensk författningssamling
Repository		One or more databases of certificates and other relevant information maintained by issuing certification authorities.
Revocation		Here AB Svenska Pass may have reason to revoke the e-ID before its normal expiration. The revoked status is published in the repository.
	GCS	AB Svenska Pass Certificate Services
	GCPSMT	AB Svenska Pass CP/CPS Management Team
	GRPS	AB Svenska Pass Relying Party Services
Qualified signature creation device	QSCD	A qualified container specifically designed to carry and protect private keys and certificates and meets the requirements laid down in the eIDAS regulation 910/2014
Secure Hash Algorithm	SHA	
Subscriber		In this document equal to "subject" and is the natural person identified in the certificate as the holder of the private key given in the certificate.

	X.500	The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, organization, etc.
	X.509	The ITU-T standard for Certificates.X.509 Version 3, refers to certificates containing or capable of containing extensions.
certificate	QC	A certificate whose primary purpose is to identify a person with a high level of assurance, where the certificate fulfils the requirements laid down in Regulation on electronic identification and trust services (eIDAS) 2012/0146(COD)..
Validation		In this document an online check by OCSP request of the validity of a certificate and the validity of any certificate in that certificate's certificate chain for the purpose of confirming that the certificate is valid at the time of the check and not revoked or expired.
Subscriber		A subscriber in this document is a natural person that is a holder of a private key corresponding to a public, and has been issued a certificate. The subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the certificate. A subscriber may apply for a AB Svenska Pass e-ID.
Secondary certificate		A certificate issued on the basis of another certificate, the primary certificate. The key usage must be consistent to the same as in the primary certificate.
Qualified electronic signature	QES	An advanced electronic signature which is based on a certificate and which is created by a QSCD.

10.2 References

[1] rfc 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework November 2003
[2] Tillitsramverket för svensk e-legitimation
http://www.elegitimationsnamnden.se/leverantor
[3] ETSI EN 319411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
[4] ISO/IEC 27001:
[5] ISO/IEC 27002:2013
[6] rfc 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile