AB Svenska Pass CA Class1 v1

Certificate Policy

Certification Practice Statement

OID 1.2.752.244.1.2.1.2.1
Date 2017-01-13
Version 1.0

Content

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“

To its subscribers, AB Svenska Pass will create authentication and “digital signature certificates” issued under AB Svenska Pass iCA Class1 v1. The private keys connected to these certificates will be stored in the 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-ID issued by AB Svenska Pass works and what obligations AB Svenska Pass has and what processes AB Svenska Pass have set within the ABSP-TS and its Certification Authorities (CAs). The document will take in consideration the AB Svenska Pass Root CA Class1 v1 and the subordinated issuing CA, AB Svenska Pass iCA Class1 v1.

This document is conform to the CP/CPS structure defined in RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

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, is using when producing its certificates. eID certificates are generated according to references defined in Appendix A.
These certificates are used in ID-Cards issued by Swedish governmental agencies

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

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. Neverless AB Svenska Pass will always be held ultimately responsible in accordance with this 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“.

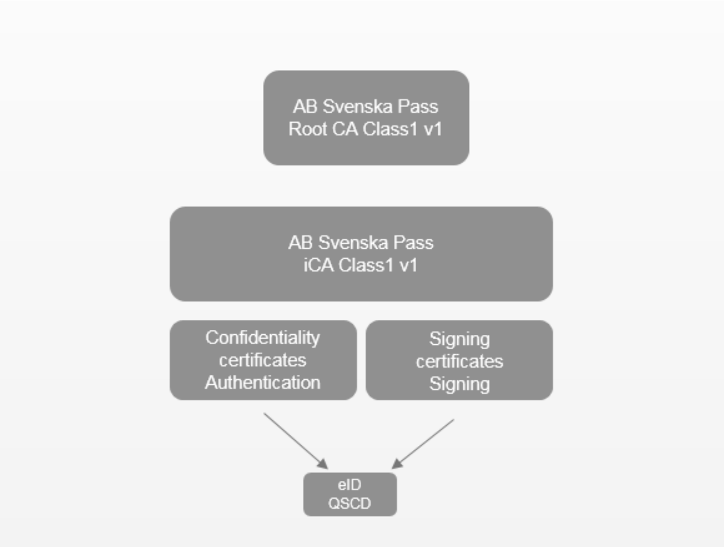
The name of this CP/CPS is AB Svenska Pass CA Certificate Practice Statement and the object identifier is 1.2.752.244.1.2.1.2.1.00

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 CP/CPS document includes the Root CA (RCA) and the iCA of the AB Svenska Pass CA Class1 v1. The RCA issued the iCA certificate and the iCA is used for issuing certificates for e-ID use. The iCA issues two types of certificates, one for authentication and the other one for signing. The authentication certificate can be used to authenticate a citizen log-in processes or authentication 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 thatall required recourses are available to meet its obligations.

AB Svenska Pass is a fully owned subsidiary of Gemalto AB

Gemalto AB
Götalandsvägen 230
svenskapass.CAinfo@gemalto.se
www.gemalto.com/sverige

1.3.2 RA

Swedish governmental agencies that issue highly trusted ID, and are appointed by AB Svenska Pass, may act as a Registration Authority (RA).

1.3.3 Subscribers

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

All subscribers have to sign an approval contract containing of AB Svenska Pass' conditions in order to use AB Svenska Pass e-ID. Subscribers under the age of 18 years must have approval from their guardians'.

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 subscribers, other CAs, contracted RAs and parties asking for authentication services as well as other providers of security services.

1.4 Certificate usage

An approved application of 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 for Electronic Signatures. The "authentication certificate" and its corresponding private key shall be used for authentication/ identification and encryption/decryption purposes.

Both "digital signature certificates" and the "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, when certificates, and their corresponding private keys are used, the certificate's usage area must be taken into consideration.

It is outwit AB Svenska Pass´ control to prevent private keys from being used for unwanted purposes or for purposes against the subscriber's intentions. It is in the subscriber's interests and responsibility to use the private keys only in trustworthy applications and reliable equipment. It is a common understanding that a subscriber never shall use the private signature key to sign data or documents that haven't first been 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 for the overall Public Key Infrastructure (PKI). The board is responsible to ensure that this CP/CPS meets the requirements in 1.5.3 and that the issuance of the ABSP e-ID is done in accordance with this CPS.

1.5.2 Contact person

Enquiries or other need for communications about this CP/CPS shall 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 that this CP/CPS meets the requirements of the ETSI EN 319411-1

1.5.4 CP/CPS approval procedures

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

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

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)

1.6 Definitions and acronyms

A list of definitions and acronyms is found in Appendix A

2. Publication and Repository Responsibilities

2.1 Repositories

The CPS, issued certificate and revocation information will be made available by AB Svenska Pass.

https://va.absvenskapass.se/CPS
http://va.absvenskapass.se/absvenskapass-class1-iCA-v1.crl
http://va.absvenskapass.se/ocsp
http://va.absvenskapass.se/absvenskapass-class1-iCA-v1-crt
http://va.absvenskapass.se/absvenskapass.class1-rootCA-v1.crt

2.2 Publication of certificate information

AB Svenska Pass will make the following information available:

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

AB Svenska Pass may publish and supply certificate information.. Subscribers will be notified that AB Svenska Pass may publish information submitted by them to accessible directories in association with certificate information. The publication of this information will be within the limits stated in sections 9.3 and 9.4. in this document.

2.3 Time or frequency of publication

Certificate information is published promptly after issuance and within 24 hours after revocation. The ABSP Repository Service are 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 are made for maintenance requirement.

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 done by a RA appointed by AB Svenska Pass. The subscriber's personal identity number is used to establish an unambiguous identity of 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 will be according to section 7.1.5. The following subscriber information is included in AB Svenska Pass e-ID certificates:

Information	Demand on content
Given Name	All of the subscriber’s given names spelled according to the register.
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 organisation.

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.

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

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

3.2.2 Authentication of individual identity

To be a subscriber of AB Svenska Pass e-ID, an application must be filled in and signed by an 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 take place by AB Svenska Pass within this 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

Responsibility for revocation is held by the RA that initially requested the certificates. RAs are obliged to provide a service to subscribers that allow them to request certificate revocation and to manage revocations related to cards being reporting lost or stolen.

AB Svenska Pass CA receives revocation requests from the RA that detail the Serial Number of the certificate, the identity of the Issuer CA and the reason for revocation.   The systems of AB Svenska Pass CA validate the authenticity and integrity of the revocation request before revoking the certificate. AB Svenska Pass CA shall keep records of all revocation requests. The records will hold information of the identity of the RA revoking the certificates and the time the revocation was done. The records are included in the audit logs of the AB Svenska Pass CA.

In the case that there is evidence of compromise or misuse, the eID will be revoked, on behalf of the subscriber, by AB Svenska Pass or an appointed RA.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate application

The AB Svenska Pass e-ID application is done by the applicant at a Swedish governmental agency, the RA administrator. 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

The AB Svenska Pass e-ID application is a 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 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

A 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. 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 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 and stores it in the QSCD of the physical ID Card.

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

- Authentication of the secured files of applications submitted by 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 requests 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 “outside”.
- Distribution of the ID Card with QSCD to the card issuer for secure physical delivery based on face-to-face recognition.

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. The activation data will be handed over by the RA administrator or be sent directly to the private address of the subscriber.

4.4 Certificate acceptance

By signing the application agreement and accepting the delivery of the ID Card with the QSCD that includes AB Svenska Pass e-ID 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 have to 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 public key and certificate usage

Prior to accepting AB Svenska Pass e-ID, a relying party is responsible to verify that the certificates is appropriate for the intended use and check the validity of the certificates, 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 shall be validated against production certificates available online:

http://va.absvenskapass.se/absvenskapass-class1-iCA-v1.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 if there is a request for it from the subscriber or in the case of any certain event that requires the revocation to take place.

4.9.1 Circumstances for revocation

There are 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 a 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 the 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 revoke the eID with it´s 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 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. Expected information and personal data will be asked for by the revocation service. The revocation is to be considered carried out after it has been confirmed by AB Svenska Pass.

A 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 take place immediately.

4.9.5 Time within which the CA must process the revocation request

AB Svenska Pass must 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 AB Svenska Pass e-ID, 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.

4.9.7 CRL issuance frequency

CRL's are issued with 1 day frequency.

4.9.8 On-line revocation/status checking availability

AB Svenska Pass provides revocation status checking in 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 is available 7 days per week, 24 hours per day except for planned maintenance.

4.11 End of subscription

The validity of the certificate issued by the iCA is five (5) years. If a subscriber chooses to unsubscribe before this period, the certificates should 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

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 is certified according to the international standard on information security control, ISO 27001.

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

Physical environment is secured by access control, mantraps and CCTV. Access to the physical environment is monitored 24/7.

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.

To prevent unwanted disclosure of sensitive data waste is disposed of in a secure manner.

5.2 Procedural Controls

The CA organization contains of a set of trusted roles, who has a specific function 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. The activities and roles are controlled in a way that no one alone should be able to have access to the CA system and its functions. For each task identified AB Svenska Pass uses M of N method, to grant access.

Trust Service Director: Responsible for the CA organization, roles and responsibilities.
Security Officer: Access to the private keys, and configuration of HSMs.
Operator: Responsible for operating the CA trustworthy systems on a day to day basis. Authorized to perform system backup and recovery. Can create and renew keys.
Auditor: Authorized to view archives and audit logs of the RCA trustworthy systems

All activities on the CA are logged, which cannot be accessed by any other role but Auditor. Auditors shall not have any other role in the CA organization.

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 personel do not have any other position in the organization that might conflict with their trusted CA role.

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 clearances as deemed appropriate.

5.3.2 Background Check Procedures

AB Svenska Pass makes the relevant checks to prospective employees by means of status reports issued by a competent authority, third-party statements or signed self-declarations.

5.3.3 Training Requirements

AB Svenska Pass personnel are trained to perform their CA trusted functions.

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

Not stipulated.

5.3.7 Independent Contractor Requirements

Not applicable

5.3.8 Documentation Supplied to Personnel

AB Svenska Pass makes available documentation to personnel, during initial training, retraining, or otherwise.

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:

- Issuance of a certificate;
- Revocation of a certificate;
- Suspension of a certificate;
- (Re)activation of a certificate;
- Automatic revocation;
- 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;
- Report of disaster recovery tests;
- Audit inspections;
- Upgrades and changes to systems, software and infrastructure;
- Security intrusions and attempts at intrusion.

AB Svenska Pass ensures that designated personnel reviews 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 in a regular manner.

5.4.3 Retention Period for Audit Log

AB Svenska Pass retains in a trustworthy manner records of digital certificates for a term as indicated under article 5.5 if this CPS.

5.4.4 Protection of Audit Log

Only trusted member 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

Not applicable.

5.5 Records Archival

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;
- Audit trails on the issuance of certificates for a period of a minimum of 10 years after issuance 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.

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.

Archives are accessible to authorized personnel of the CA.

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

Only the AB Svenska Pass member of staff assigned with the 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.

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

AB Svenska Pass retains records in electronic or in paper-based format.

5.6 Key Changeover

A subscriber private key cannot be renewed but requires a new application of an ID Card and 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

A business continuity plan has been implemented to ensure business continuity following a natural or other disaster.
All such measures are implemented based on ISO 27001.

AB Svenska Pass specifies the recovery procedures used in case computing resources, software, and/or data are corrupted or suspected of being 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.

In case of suspected or known compromise of a private key, the ABSP Crisis procedures are 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 eID Repository Website or through the eID CRL Website.

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.

5.8 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 like subscribers, relying parties and other directly affected entities. For planned actions termination plans will be set up in advance to minimise any dysfunctions.

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-ID connected to that RA.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA and RA use a trustworthy process for the generation of its CA private key according to a documented procedure.
The key pairs for the subordinated issuing CAs of the AB Svenska Pass CA Class1 v1 (Issuing CA Keys) have been generated in an HSM that meets at least FIPS 140-2 requirements.

Before 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. The access to the secured place with the non-initialized cards and devices is restricted in such a way that two persons need to be present when managing the cards.

The generation of private keys and personalization of QSCD equipped cards are done in batches and the batches are used 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 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 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 provided to subscriber

QSCD equipped cards are distributed via the ID Card issuer.

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

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

6.1.4 Publicity of certification issuer's public key

The root certificate and issuing certificates are available to relying parties.

6.1.5 Key sizes

The CAs' issuer keys are generated as RSA keys with a minimum length of 4096 bits. The subscribers' and operators' RSA keys are generated with a minimum length of 2048 bits.

6.2 Private key protection and cryptographic module engineering controls

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 rated to at least FIPS 140-2. 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.

6.2.1 Cryptographic module standards and controls

Hardware protected private keys are created and stored in QSCD equipped cards. The keys will be generated and protected in a cryptographic module rated to at least FIPS 140-2 regarding hardware and card OS.

6.2.8 Method of activating private key

A card holder must be authenticated to the QSCD before the activation of the private keys in the AB Svenska Pass e-ID. This authentication is done by using a PUK as activation data to each private key.

6.3 Other aspects of key pair management

Initialization, personalization and generation of private keys for QSCD equipped cards takes place in a well-protected area. Access to the area is granted individually and at least two persons have to be present in the area at all times. All access to the area is logged.

The production logs for production of the QSCD includes information of all orders from RA and are connected to personal data of the subscriber and chip identification, card serial number and certificate serial numbers that have been generated in the production processes.

Routines are established to verify that visual information on the hardware device are corresponding to the information in AB Svenska Pass e-ID connected to the private keys protected by the QSCD.

The life time of AB Svenska Pass e-ID is linked to the expiration day of the physical ID Card.

6.4. Activation data

6.4.1 Activation data generation and installation

All subscribers' private keys are protected by PINs of at least six digits and a PUK of eight digits.

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 Protection and life-cycle of activation data

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.

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.

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 CPS.

6.5.2 Computer security rating

Not applicable

6.6 Life cycle technical controls

All hardware and software procured for operating an Issuing CA must be purchased in a manner which will mitigate the risk that any particular component could be tampered with, such as random selection of specific components. 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 causing it to be shipped or delivered via controlled methods. Issuing CA equipment shall not have installed any application or component software that is not part of the Issuing CA configuration. 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.

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

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.

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, suspension, un-suspension and revocation.
- The CA web site provides for encrypted connections through the Secure Socket Layer (SSL) protocol and anti-virus protection.
- 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.

6.8 Time-stamping

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

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate profile

The contents definition of a certificate, in other words the certificate profile, defines the fields in a certificate. The certificate profile of the certificates 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”.

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

CA Name	The name of the CA
CA Standard	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

The 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 document AB Svenska Pass eID Naming and Profile Document.

7.1.3 Cryptographic algorithm object identifiers

Root CA Signature algorithm: ecdsa-with-SHA384
Sub CA Signature algorithm: ecdsa-with-SHA256

7.1.4 Name forms

Every 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/CPS) where this 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 CRL 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

8.1 Frequency or circumstances of assessment

A compliance audit has taken place by the eID board, which has also approved the internal compliance auditor. During a 3-year period the CA shall be annually audited by an internal independent control function to ensure compliance.

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

8.2 Identity/qualifications of assessor

The audit services are to 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 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 (“Valfrihetssytem 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 fullfil its responsibilities according to this 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 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

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

AB Svenska Pass will treat the following information as being private:

a) Application and reception forms
b) PUK
c) Correspondence between AB Svenska Pass, RA and card manufacturer.
d) Logged events.

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

Private keys and corresponding public keys are the sole properties of the rightful subscriber defined in the certificates.

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 CPS, when issuing and managing AB Svenska Pass e-ID and will ensure that the RA operating on its behalf comply with the relevant provisions of this CPS. AB Svenska Pass will take commercially reasonable measures to ensure that subscribers and relying parties 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 CPS. AB Svenska Pass liability is limited to it´s contractual agreements with the subscriber.

9.6.2 RA representations and warranties

AB Svenska Pass requires that all RA comply with the relevant provisions of this 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 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 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 the information with activation date (PIN/PUK) has not been share with any other person, 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 will require that relying parties comply with all the relevant provisions of this CPS. Prior to accepting a AB Svenska Pass e-ID, a relying party is responsible to:

- Verify that the certificate is appropriate for the intended use.
- Check the validity of the certificate, i.e. verify the validity dates and the validity of the certificate and issuance signatures.
- Check the status of the certificate against the appropriate OCSP responder in accordance with the requirements stated in this 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.

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 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 eID repository. Amendments to this CP/CPS become effective after publication in the eID 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

AB Svenska Pass will define in any applicable agreement the appropriate provisions to handle notices.

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/CPS.

9.12.2 Notification mechanism and period

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 Svensk Pass TS services. The period of time that affected parties have to conform to the change will be defined in the notification.

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 CPS, ABSP-TSEB will assign a new object Identifier (OID) for the new CPS.

9.13 Dispute resolution procedures

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

9.14 Governing law

Swedish law shall apply to the interpretation of this 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.

Appendix A

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 indentifying the signatory; c) it is created using means that the signatory can maintain under his sole control; and d) 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).
PKCS #10		A certificate request format or syntax managed and edited by RSA Laboratories. It is a standard describing syntax for a request for certification of a public key, a name, and possibly a set of attributes.
PKCS#15		Cryptographic Token Information Format Standard from RSA Laboratories. PKCS #15 establishes a standard that enables users in to use cryptographic tokens to identify themselves to multiple, standards-aware applications, regardless of the application's cryptoki (or other token interface) provider.
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.
	RSA	
	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
Secure signature creation device	QSCD	A secure container specifically designed to carry and protect private keys and certificates and meets the requirements laid down in annex III of the Directive 1999/93/EC.
	SHA-1	
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.
TeleTrusT Token		A hardware device with two key pairs used for signing electronic documents, electronic identification and key encryption. Each private key is secured by a separate PIN. The prototype version was published 1987 and influenced the chip development in the smart card industry. See E-ID which is the Swedish name for such device.

	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 meets the requirements laid down in annex I of the Directive 199/93/EC and is provided by CSP who fulfils the requirements laid down in annex II of the Directive 199/93/EC.
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.
electronic signature	QES	An advanced electronic signature which is based on a certificate and which is created by a QSCD, as defined in article 5.1 of the Directive 1999/93/EC.

References

RFC 2560
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
Provided by IETF, http://www.ietf.org.
RFC 3647
An IETF framework document providing a list of topics that potentially need to be covered in a Certificate policy or a certification practice statement.
Provided by IETF, http://www.ietf.org.
RFC 5280
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Provided by IETF, http://www.ietf.org.
ETSI EN 319411-1: 4-5-7
Policy and security requirements for trust service providers issuing certificates, Part1: General requirements
Provided by ETSI, http://www.etsi.org.
Tillitsramverket för svensk e-legitimation
http://www.elegitimationsnamnden.se/leverantor