Certification Practice Statement (CPS)

Versions			
Ver.no	Date	Name	Description
0.1	2025-10-02	CAA, Linda Fagerholm	English version created
1.0	2025-10-08	CEO, Christina Pettersson	Document approved

Roles and responsibilities of the document			
Author:	CAA, Linda Fagerholm	Date:	2025-10-02
Reviewed by:	Product owner CA, Katarina Eriksson	Date:	2025-10-03
Approved by:	CEO, Christina Pettersson	Date:	2025-10-08

Disclaimer

This document is a translation from the original Swedish version into English. In case of any discrepancies, ambiguities, or disputes regarding interpretation, the Swedish version shall prevail.

Expisoft AB, CA Tjänsten, Box 2934, CA SE-187 29 Täby, Sweden
+46 (0)8 123 502 80, certifikat@expisoft.se, www.expisoft.se

Approved by:	CEO, Christina Pettersson	Date:	2025-10-08

Table of contents

Approved by:	CEO, Christina Pettersson	Date:	2025-10-08

1 Introduction

This document is a Certification Practice Statement (CPS) that is owned and maintained by Expisoft AB, hereinafter referred to as the “Issuer". This Certification Practice Statement describes how the Issuer meets the requirements set out in the Certificate Policies covered by this declaration (see section 1.1).

This document is relevant for the Issuer, the RA function and its personnel, resellers of the Issuer’s certificate products, requesters within a customer organization, relying parties, and e-service identification holders.

The Certification Practice Statement describes the procedures and processes applied by the Issuer when issuing certificates. Separate documents, Certificate Policies, describe the certificates themselves and the requirements that the certificates correspond to.

By reviewing both the Certificate Policies and this Certification Practice Statement, external parties can form an understanding of the security level of the certificates issued.

Both the Certificate Policies and Certification Practice Statement follow and are structured according to the recommendations in IETF RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" and RFC 7382 "Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)."

1.1 Overview

This Certification Practice Statement applies to all certificates issued by the Issuer. Examples of certificates covered include:

OID: 1.2.752.54.9.2.25.3
Product name: e-Tjänstelegitimation Kort
CA instance: ExpiTrust e-Tjanstelegitimationer kort CA v4

OID: 1.2.752.54.9.2.26.3
Product name: E-tjänstelegitimation fil
CA instance: ExpiTrust e-Tjanstelegitimation CA v3

OID: 1.2.752.54.9.2.13.2
Product name: EID Funktion/Organisation
CA instance: ExpiTrust EID CA v4

1.2 Document name and identification

All issued certificates shall contain Object Identifiers (OIDs) corresponding to their Certificate Policy, certifying that the Issuer has issued and validated the certificates in accordance with the established procedures.

1.3 PKI Parties and their responsibility

Described in the respective Certificate Policy.

1.4 Certificate (e-identification) usage

Described in the respective Certificate Policy.

1.5 Document administration

1.5.1 Organization responsible for administering this document

The issuer Expisoft AB is responsible for the management, administration, and maintenance of this Certification Practice Statement. Questions regarding this Certification Practice Statement should be addressed to:

Expisoft AB
CA-Tjänsten
Box 2934
187 29 Täby
Sweden

E-mail: certifikat@expisoft.se
Phone: +46 (0)8 123 502 80

1.5.2 Contact person

The person responsible for the CA service is to be contacted in writing using the address information provided above.

1.5.3 Person who determines Certificate Practice Statement suitability based on Certificate Policies

The role of the Certificate Authority Administrator (CAA) (see chapter 5.2.1) is responsible for ensuring the suitability and applicability of this Certification Practice Statement with respect to the Certificate Policies covered.

1.5.4 Approval procedure for this Certificate Practice Statement

The role of Certificate Authority Administrator (CAA) (see chapter 5.2.1) is responsible for the approval process of this document.

1.6 Definitions and acronyms

See chapter 10 for definitions and abbreviations used in this document.

2 Publication and repository responsibilities

2.1 Storage locations

Information related to the Issuer's CA service, this Certification Practice Statement, and the relevant policies is published on the Issuer's website. The information is available at https://www.expisoft.se/ and https://eid.expisoft.se/.

2.2 Publication of certificate-related information

The Issuer provides information in accordance with the respective Certificate Policy. Certificate Revocation Lists (CRLs) and root certificates are available at: https://eid.expisoft.se/.

2.3 Times and frequencies of publication

Described in the respective Certificate Policy.

2.4 Authorization control for storage locations

Described in the respective Certificate Policy.

3 Identification and authentication (I&A)

3.1 Naming

3.1.1 Types of names

Described in the respective Certificate Policy.

3.1.2 Need for meaningful names

Described in the respective Certificate Policy.

3.1.3 Anonymous or pseudonymous e-identification holders

Described in the respective Certificate Policy.

3.1.4 Rules for interpreting different name formats

Described in the respective Certificate Policy.

3.1.5 Unique names

Described in the respective Certificate Policy.

3.1.6 Recognition, authentication, and the role of trademarks

Described in the respective Certificate Policy.

3.2 Initial identity validation

3.2.1 Method to prove possession of the private key

In cases where the Issuer generates the key pair and creates a file-based certificate, a copy of the p12 file is stored by the Issuer. This file contains both the private and the public key. In cases where a Requester has generated the key pair themselves and requests a certificate through a CSR, ownership is verified by the fact that the CSR is signed with the Requester's private key. In this way, the Issuer can be certain that the certificate request comes from the holder of the private key.

3.2.2 Authentication of the organization's identity

The Issuer's RA function verifies, via the Swedish Companies Registration Office (Bolagsverket), the Swedish Tax Agency (Skatteverket), and publicly available and reliable information on the internet, that the organization/company exists with the correct Swedish organization number and accounting history. The position of the individual who signed the order is also verified. When necessary, the information is supplemented, for example, through telephone calls to an independent party who can confirm the individual's role or the organization's identity.

3.2.3 Authentication of the individual's identity

The Issuer's RA function verifies that the Requester is an individual (and not a role, e.g., a support department) as well as the position details of the person who signed the order. Furthermore, PIN letters are delivered either by registered mail (requiring valid identification upon receipt) or digitally, when the order has been signed by an authorized person using Swedish Mobile BankID.

3.2.4 Unverified data about the e-identification holder

Described in the respective Certificate Policy.

3.2.5 Validation of authorization of Agent

All Agents approved by the Issuer have Administrators with their own personal e-identifications. The Administrator's e-identification is used to identify the Agent when logging into the Issuer's web portal to request certificates either for the Agent's own organization or for the organization's customers (as a reseller). Through the Issuer's web portal, the Agent's Administrators can manage, monitor, request, and revoke certificates for their respective customer groups.

3.2.6 Criteria for collaboration

Described in the respective Certificate Policy.

3.3 Verifying the identity for requests of key renewals

Not applicable. A request to renew a key pair is regarded as a new order and follows the procedures described in chapter 4.1.

3.3.1 Identification and authentication in the renewal of key pairs for a valid certificate

Not applicable. A request to renew a key pair is regarded as a new order and follows the procedures described in chapter 4.1.

3.3.2 Identification and authentication in the renewal of key pairs after certificate revocation

Not applicable. A request to renew a key pair is regarded as a new order and follows the procedures described in chapter 4.1.

3.4 Verifying identity for revocation requests

Both the certificate holder and the Requester can revoke certificates directly via the Issuer's web page (this requires access to the unique identifier from the PIN letter). When revocation is requested by phone, the certificate holder's identity is verified by checking the PIN letter and performing a callback. Once it has been confirmed that the revocation request is legitimate, the certificate is revoked without delay.

4 Certificate life-cycle operational requirements

4.1 Order of e-identifications

4.1.1 Who can order an e-identification

Described in the respective Certificate Policy.

4.1.2 Order procedure and responsibility

Described in the respective Certificate Policy.

4.1.3 Identification with Swedish Mobile BankID

Identification using Swedish Mobile BankID can be performed by an authorized representative of the ordering organization for the purpose of granting the Requester a power of attorney to place an order on behalf of the organization.

4.2 E-identification order processing

All orders are registered by the Requester in the Issuer's web portal, ensuring that orders are kept separate from one another. The personnel at the Issuer handling the orders are all certified by the Issuer. In addition, the "four-eyes principle" is applied, meaning that two authorized individuals participate in the issuance of all certificates to ensure that no manual errors occur during the issuance process.

4.2.1 Identification and authentication

Described in the respective Certificate Policy.

4.2.2 Approval or rejection of an e-identification order

Described in the respective certificate policy. The Issuer notifies the Requester via email (for traceability reasons) of the reason why an order has been rejected and what is required for the order to be approved.

4.2.3 Processing time for certificate and e-identification request

Described in the respective Certificate Policy.

4.3 Certificate issuance

4.3.1 Activities during certificate issuance

The certificate issuance process begins when a person with the RA role logs into the CA systems and authenticates using a personal, valid e-identification. The information in the application/order is validated in accordance with chapter 3.2 of the corresponding Certificate Policy. A new key pair is generated unless the customer has submitted a CSR order where the key pair has been generated by the customer, or if the keys are already stored on a smart card. Certificates are issued according to the order (either as a file or ready to be placed on a smart card). During the certificate issuance process, two trusted individuals (at least one of whom holds the RA role) participate to minimize the risk of manual errors. If the order concerns card-based certificates, the certificate is loaded onto the smart card (personalization).

4.3.2 Issuer's notification to the Requester regarding issuance of e-identification

The Requester is notified in writing via email that the ordered certificate has been issued, and a PIN letter containing the unique identifier is delivered to the Requester either as a PostNord registered Letter (REK) or digitally via the web portal. Once the Requester has access to the unique identifier, they can download their certificate through a self-service function. If a smart card certificate has been ordered, it is delivered to the Requester by mail, separately from the PIN letter.

4.4 E-identification/ certificate acceptance

4.4.1 Procedures that establish acceptance of issued e-identification

Described in the respective Certificate Policy.

4.4.2 Publication of issued e-identification by the certificate issuer

In the Issuer's web portal, Requesters can log in and retrieve their ordered certificates (public part). For certain certificate policies, the Issuer uses a public LDAP directory containing certificates and revocation lists in accordance with the certificate policy.

4.4.3 The Issuer's information to third parties about issued e-identification

Described in the respective Certificate Policy.

4.5 Key pair and certificate usage

4.5.1 Use of the private key associated with the e-identification

Described in the respective Certificate Policy.

4.5.2 Use of the public key associated with the e-identification

Described in the respective Certificate Policy.

4.6 E-identification renewal

Described in the respective Certificate Policy.

4.6.1 Reasons for renewal of the e-identification

Described in the respective Certificate Policy.

4.6.2 Who can request renewal

Described in the respective Certificate Policy.

4.6.3 Handling of requests for renewal of the e-identification

Described in the respective Certificate Policy.

4.6.4 Notification to the Requester regarding the new issuance of the e-identification

Described in the respective Certificate Policy.

4.6.5 Procedures that establish the acceptance of the renewed e-identification

Described in the respective Certificate Policy.

4.6.6 The Issuer's publication of the renewed e-identification

Described in the respective Certificate Policy.

4.6.7 The Issuer's notification to other parties regarding the issuance of the e-identification

Described in the respective Certificate Policy.

4.7 Renewal of the certificate key pair

Described in the respective Certificate Policy.

4.7.1 Reasons for renewal of the certificate keys

Described in the respective Certificate Policy.

4.7.2 Who can request a renewal of the certificate keys

Described in the respective Certificate Policy.

4.7.3 Handling of requests for renewal of the certificate's keys

Described in the respective Certificate Policy.

4.7.4 Notification to the Requester regarding the new issuance of the certificate

Described in the respective Certificate Policy.

4.7.5 Procedures establishing acceptance of the certificate

Described in the respective Certificate Policy.

4.7.6 The Issuer's publication of certificates with new keys

Described in the respective Certificate Policy.

4.7.7 The Issuer's notification to other parties regarding the issuance of keys

Described in the respective Certificate Policy.

4.8 Certificate modification

Described in the respective Certificate Policy.

4.8.1 Reasons for modifications of a certificate

Described in the respective Certificate Policy.

4.8.2 Who can request modification of a certificate

Described in the respective Certificate Policy.

4.8.3 Handling of requests for modification of a certificate

Described in the respective Certificate Policy.

4.8.4 Notification to the Requester regarding modification of a certificate

Described in the respective Certificate Policy.

4.8.5 Procedures that establish the acceptance of a modified certificate

Described in the respective Certificate Policy.

4.8.6 The Issuer's publication of the modified certificate

Described in the respective Certificate Policy.

4.8.7 The Issuer's notification to other parties regarding the certificate modification

Described in the respective Certificate Policy.

4.9 Certificate revocation and suspension

The Issuer provides a web service where certificate holders can revoke their own certificates. Alternatively, certificate holders may contact the CA service's support function to request certificate revocation. Revocation lists are published via an OCSP service.

4.9.1 Reason for certificate revocation

Described in the respective Certificate Policy.

4.9.2 Who can request a revocation

Described in the respective Certificate Policy.

4.9.3 Procedure for revocation request

The Certificate holder or Requester can revoke a certificate themselves (for any reason) via the Issuer's website, provided they have access to the certificate's unique identifier (found in the PIN letter). For revocation requests made by phone, the identity of the requester is verified in accordance with chapter 3.4. The Issuer may also decide to revoke a certificate even if identification cannot be performed, in cases where there is a risk of misuse of the e-identification/certificate. Received revocation requests are archived along with the following information:

- Date and time
- Information on who ordered the revocation
- Reason for revocation (when the Issuer revokes the certificate)
- Executing person (in the case of manual revocation)

4.9.4 Processing time for revocation requests

Described in the respective Certificate Policy.

4.9.5 Time within which the CA must process revocation requests

Described in the respective certificate policy. The Issuer provides a web-based revocation service that is available 24/7. Alternatively, revocation can be carried out via the Issuer's support function from 09:00 to 16:00 on weekdays, excluding public holidays.

4.9.6 Requirements for the Relying party in case of a revocation request

Described in the respective Certificate Policy.

4.9.7 Frequency of publication of revocation lists (CRL)

The Issuer creates and publishes revocation lists once per hour, around the clock, with a validity period of 24 hours. A new revocation list is also created and published immediately when the CA service receives and processes a revocation request. This ensures that there is always a current and up-to-date revocation list available for retrieval and/or use in an OCSP query.

4.9.8 Maximum delay of publication of revocation lists (CRL)

The Issuer issues new revocation lists every hour, and within a few minutes they are available on both internal and external CDPs. If more than an hour passes since the previous revocation list was published, an alert is sent to the Issuer's operations organization so that any issues can be resolved and revocation lists can be published correctly again. If the delay exceeds a certain threshold, a continuity plan for the CA service is activated.

4.9.9 Online revocation request and status/revocation check

At the Issuer, these functions are included in the base service at no additional cost for relying parties. All responses to OCSP requests are signed by the OCSP server, which holds its own certificate issued by the CA service. The OCSP service is regularly updated using the CA service's revocation list, published according to the time intervals specified in chapter 4.9.7. The Issuer operates two OCSP servers for redundancy and load balancing, one in its own data center and one at a different location.

4.10 Certificate status services

4.10.1 Properties

Revocation lists are published in the Issuer's public registry/directory according to the criteria described in the respective Certificate Policy. Both the CRL and the OCSP service are freely accessible to all relying parties.

4.10.2 Availability

The Issuer uses dual OCSP sites to ensure access even if one site experiences an outage. CRLs have a validity period of 24 hours, but a new CRL is issued at least every hour. This means that even in the event of a disruption in the issuance of a new CRL, there is a 23-hour window before the old CRL file expires.

4.11 End of e-identification subscription

Described in the respective Certificate Policy.

4.12 Key escrow and recovery

Described in the respective Certificate Policy.

5 Facility, management, and operational controls

5.1 Physical security controls

5.1.1 Physical location and structure

Described in the respective Certificate Policy. The Issuer meets all the requirements of the respective Certificate Policy regarding the CA system's operational environment.

5.1.2 Physical access

Physical access to the CA system's operational environment is protected by an alarmed door with two-factor authentication, digital logs, and a manual logbook. The operational environment is located within a secure enclosure equipped with dual padlocks. Access also requires the presence of at least two trusted people. A continuity plan is in place, and deviation reporting must be carried out if the two-people requirement is not met.

5.1.3 Power supply and cooling

The Issuer uses a combination of UPS and a fuel-powered generator to ensure continuous operation for at least 24 hours during a power outage. The generator's functionality is tested four times a year by a subcontractor, with written test reports. The Issuer conducts a complete grid disconnect test at least once a year, also with a written test report.

5.1.4 Water exposure

The CA system's operational environment at the Issuer is equipped with flood alarm.

5.1.5 Fire protection

The CA system's operational environment at the Issuer is equipped with fire alarm.

5.1.6 Storage of media

The CA system's storage media are kept locked together with the rest of the CA system. The hardware is redundant to reduce the risk of data loss in the event of a failure. The Issuer stores encrypted backups of the CA systems both on a separate backup server and on an offsite backup. The decryption keys for these copies are kept in a location separate from the backups themselves. Archive copies containing CA information are temporarily stored on a separate tape robot before being placed in a dedicated fireproof safe (within the Issuer's premises) to which only trusted personnel have access.

5.1.7 Waste management

The Issuer destroys sensitive material by engaging a separate company specialized in the destruction of data disks. The sensitive material to be destroyed is never left unattended from the moment it leaves the Issuer's premises until it has been destroyed.

5.1.8 Backup at another location

Backups of the CA systems are stored on an offsite backup. Archive copies containing CA information are stored in a dedicated fireproof safety cabinet, separate from the CA system.

5.2 Procedural controls of the CA function

The Issuer has documented policies and procedures for certificate issuance, with version control to ensure that updates to the procedures can be easily tracked and distributed.

5.2.1 Trusted roles

Described in the respective Certificate Policy. The Issuer maintains the roles specified in the policy, with separate role descriptions available.

5.2.2 Requirements for number of people per task

Described in the respective certificate policy. The Issuer applies dual control in the situations listed in the policy. “Handling of logs” refers, for example, to deleting or purging old log entries (older than the required retention and archiving period). Performing a backup of the CA system that includes logs is not considered handling of logs. In cases where the requirement for multiple people is waived due to critical events and in accordance with the CA service’s continuity plan, the deviation is thoroughly documented for historical record and review.

5.2.3 Identification and authentication for each role

At the Issuer, each individual associated with the CA function has a CA role-specific smart card credential, which is used for authentication when performing operations in the CA system.

5.2.4 Roles that require task separation

Described in the respective Certificate Policy.

5.3 Personnel controls

5.3.1 Requirements for competence, experience and formal qualifications

Described in the respective Certificate Policy.

5.3.2 Background check

All permanent staff at the Issuer undergo background checks prior to employment. For temporary consultants, the checks may be less extensive, but this is compensated by restricting their privileges and access to sensitive systems. RA administrators acknowledge receipt of information by confirming that they have read, understood, and will comply with the instructions and procedures (including when these are updated).

5.3.3 Training requirements

Employees at the Issuer receive training based on their individual needs and roles and are monitored/reviewed during audits or inspections.

5.3.4 Requirements for competence development

All personnel at the Issuer receive necessary training and skill development when systems or procedures change. This can be provided through written or oral instructions, or via continuing education/training for the employee.

5.3.5 Job rotation

Described in the respective Certificate Policy.

5.3.6 Disciplinary actions for unauthorized activities

The severity of the unauthorized activity determines the sanction or action taken. Examples of actions include a written warning, termination of employment, or a police report.

5.3.7 Requirements for supplier independence

Described in the respective Certificate Policy.

5.3.8 Documentation for personnel

The Issuer has documented procedures and instructions for various operations carried out in connection with the issuance of certificates. During recurring internal reviews and audits, an assessment is made as to whether the existing instructions are sufficient and satisfactory, or if they need to be updated.

5.4 Audit logging procedures

5.4.1 Types of events to be recorded

Described in the respective Certificate Policy.

5.4.2 Frequency of log analysis

At the Issuer, the CAA role reviews security logs to detect security-related incidents. This is done either on a regular basis or when there is suspicion of an incident. Operational logs are monitored and checked as needed by the SA role.

5.4.3 Retention period for logs

Described in the respective Certificate Policy. The logs are stored on tape, and the tapes are kept in a fireproof safety cabinet for 5-15 years, depending on their content.

5.4.4 Protection of logs

At the Issuer, logs are protected against unauthorized modification through the logical protection mechanisms in the operating systems, as well as by the fact that the CA systems themselves are only physically and logically accessible to authorized personnel. All logs/events are provided with integrity protection and individual timestamps.

5.4.5 Backup of logs

Backups are performed of the entire CA system, which also includes the logs. Furthermore, archival copies, which also contain logs, are stored. See chapter 5.5.

5.4.6 Log collection system

The Issuer does not use any specific system for log collection.

5.4.7 Notification to the originator of the log event

For security reasons, no message is displayed to the person who triggered a log event.

In the event that a person with malicious intent interferes with the system, it is preferable that they are unaware that the system logs the actions performed.

5.4.8 Vulnerability assessment

The Issuer conducts a risk and vulnerability analysis of the CA operations as needed, but at least once a year.

5.5 Records archival

5.5.1 Type of information to be archived

Described in the respective Certificate Policy.

5.5.2 Retention period for archives

Described in the respective Certificate Policy.

5.5.3 Protection of archives

According to the respective Certificate Policy. Archived material is stored in a fireproof security cabinet. The cabinet is located in a restricted area monitored by alarms and cameras, with strict visitor management.

5.5.4 Backup of archives

Described in the respective Certificate Policy.

5.5.5 Requirements for timestamping of archived documents

At the Issuer, the time of archiving is recorded both in the logs, as described in chapter 5.4.1, and by naming the archive copies with the date included in the filename.

5.6 CA key changeover

Relying parties known to the Issuer are contacted by the Issuer well in advance of the transition to a new CA key.

5.7 Compromise and disaster recovery

5.7.1 Procedures for major incidents

Described in the respective Certificate Policy.

5.7.2 Damage to computers, software, and/or data

The Issuer continuously creates backups of both information and systems. In the event of a suspected compromise of a private key, the procedure described in the respective Certificate Policy is followed.

5.7.3 Disaster recovery and business continuity capability

At the Issuer, the continuity plan focuses on ensuring that operations can be resumed as soon as possible, although this depends on the extent of the disaster. The plan is reviewed and updated at least annually to ensure that it remains current and reflects the operational environment of the CA service.

The Security Officer for the CA service (the ISSO role) has overall responsibility for assessing the security situation and determining the measures to be taken.

5.8 CA termination

Described in the respective Certificate Policy.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Described in the respective Certificate Policy.

6.1.1.1 Issuer Keys for signing certificates and revocation lists

The generation and management of new issuer keys are carried out in accordance with the respective Certificate Policy, also access to the HSM module requires two authorized people.

6.1.1.2 Key pairs for e-identification holders

Described in the respective Certificate Policy.

6.1.2 Delivery of the private key to the e-identification holder

The delivery of card-based certificates from the Issuer is carried out by postal delivery.

The delivery of file-based certificates is carried out through the Issuer's web portal directly to the Requester.

The activation information for the certificate along with the associated PIN are sent by registered mail to the Requester, alternatively, the PIN letter can be obtained via the web portal.

6.1.3 Delivery of the public key to the certificate issuer

In cases where the Requester uses a CSR, the Issuer receives the public key when the Requester uploads the key to the web portal in connection with the order.

6.1.4 Delivery of the CA's public keys to relying parties

Public issuer keys are available for download from the Issuer's website. In some cases, the CA certificate is delivered together with the certificate, for example on a smart card, and can be read from there.

6.1.5 Key size

Described in the respective Certificate Policy.

6.1.6 Parameters for public key generation and quality control

Described in the respective Certificate Policy.

6.1.7 Purpose of key usage (the key usage field of certificates)

Described in the respective Certificate Policy.

6.2 Private key protection and cryptographic module engineering controls

Described in the respective Certificate Policy.

6.2.1 Standard and procedure for the use of a cryptographic module

The Issuer uses HSM modules certified according to CC EAL4+ and FIPS 140-2 Level 3. The CA service uses HSM modules for, among other things, the generation, storage, and use of the Issuer's keys. Hardware redundancy is applied by using two mirrored HSM modules. The private keys of the issued certificates may be stored and used on the holder's computer, phone, or other device (PKCS#12), or on a smart card (PKCS#15).

6.2.2 Requirement for multiple people to manage a private key (n of m)

Described in the respective Certificate Policy.

6.2.3 Key escrow of the private Issuer key

Described in the respective Certificate Policy.

6.2.4 Backup of the private Issuer key

Described in the respective Certificate Policy. The CA service's private keys cannot be extracted from the HSM module; therefore, a backup is created at the time of generation of the private issuer key. The backup is encrypted with AES 256 and stored on a USB drive. The decryption key is physically printed on paper and kept in an envelope together with the USB drive containing the backup. These are stored in a locked and alarmed security cabinet, accessible only to a small number of trusted personnel.

6.2.5 Archiving the private Issuer key

Described in the respective Certificate Policy.

6.2.6 Transport of the private Issuer key to and from the cryptographic module

The private issuer key is generated in the cryptographic module specified in chapter 6.2.7 and never leaves the module except when archiving a backup or if the key is to be transferred to a new cryptographic module. Export is made to external storage media (USB), where the private key is stored in encrypted form.

6.2.7 Storage of the private Issuer key in the cryptographic module

Described in the respective Certificate Policy.

6.2.8 Method for activating the private Issuer key

Activation of the CA service's private keys for root certificates requires the involvement of two people and is performed only when new CA certificates are to be created. Access to the HSM module requires a specific PIN, and additional activation information is then required to activate the private issuer key.

6.2.9 Method for deactivating the private Issuer key

The CA service's private issuer key is deactivated by being destroyed, see chapter 6.2.10.

6.2.10 Method for destroying the private Issuer key

The CA service's private issuer key is destroyed when its validity period has expired or if it has been revoked. This is done by permanently deleting the private key from the HSM and destroying the backup copy of the private key. The backup copy is destroyed by permanently destroying the storage media used. This process is carried out in the presence and under the supervision of at least two authorized persons. The process is documented with regard to the procedures performed and the persons present. However, issuer keys must not be destroyed if doing so would conflict with the archiving requirements in the respective Certificate Policy or with requirements in other applicable legislation.

6.2.11 Security evaluation of the cryptographic module

Described in the respective Certificate Policy.

6.3 Other aspects of key pair management

Described in the respective Certificate Policy.

6.3.1 Archiving the public key

Described in the respective Certificate Policy.

6.3.2 Validity period for e-identifications and key pairs

Described in the respective Certificate Policy.

6.3.3 Responsibility for the PIN/PUK and passwords of the e-identification

Described in the respective Certificate Policy.

6.4 Activation data

6.4.1 Generation and installation of activation data

Described in the respective Certificate Policy.

6.4.2 Protection of activation data

At the Issuer, activation information is protected against theft and fire by being locked in a dedicated secure cabinet, accessible only to a small number of trusted personnel.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

The Issuer's operational environment for the CA systems is set up in accordance with the respective Certificate Policy. Personal smart cards are used for logging into the CA systems, and both logins and actions performed in the systems are logged. Certain operations require dual control, as specified in chapter 5.2.2 of the Certificate Policies.

6.5.1 Special IT security requirements

Described in the respective Certificate Policy.

6.6 Life cycle security controls

6.6.1 Security requirements for system development

At the Issuer, all software development is carried out according to the Issuer's development model. Each development workstation is equipped with antivirus software and other enabled security features. Logging into the development workstations requires strong authentication. Production code is built on a dedicated build machine. All new versions of the CA service software are also tested in a separate acceptance test environment before being deployed to production.

6.6.2 Security requirements for security administration

Described in the respective Certificate Policy.

6.7 Network security controls

Described in the respective Certificate Policy.

6.8 Timestamping

Unified time across the entire CA system. Time is synchronized using GPS and cannot be influenced externally.

7 Certificate, CRL, and OCSP profiles

Described in the respective Certificate Policy.

8 Compliance audit and other assessments

8.1 Frequency and circumstances of review

Described in the respective Certificate Policy.

8.2 Identity/qualifications of auditors

Described in the respective Certificate Policy.

8.3 Auditor's relationship to the assessed entity

Described in the respective Certificate Policy.

8.4 Areas for audit

Described in the respective Certificate Policy.

8.5 Actions taken as a result of a detected deficiency

Described in the respective Certificate Policy.

8.6 Communication of audit results

Described in the respective Certificate Policy.

9 Other business and legal matters

9.1 Fees

9.1.1 Fees for the issuance of e-identifications

Prices for e-identifications are specified in the web portal https://eid.expisoft.se, or according to separate agreements with the customer organization.

9.1.2 Fees for access to certificates

Not applicable.

9.1.3 Fees for access to revocation information

Described in the respective Certificate Policy.

9.1.4 Fees for other services

Not applicable.

9.1.5 Refund policy

Not applicable.

9.2 Financial responsibility

9.2.1 Insurance coverage

Not applicable.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance and warranties for end users

Not applicable.

9.3 Confidentiality of business information

Not applicable. Not governed by this document.

9.3.1 Scope of confidential information

Not applicable.

9.3.2 Information not considered confidential

Not applicable.

9.3.3 Responsibility for protecting confidential information

Not applicable.

9.4 Privacy of personal information

Not applicable. Not governed by this document.

9.4.1 Confidentiality plan

Not applicable.

9.4.2 Information treated as private

Not applicable.

9.4.3 Information not considered private

Not applicable.

9.4.4 Responsibility for protecting private information

Not applicable.

9.4.5 Notice and consent for the use of private information

Not applicable.

9.4.6 Disclosure in accordance with legal and administrative processes

Not applicable.

9.4.7 Other circumstances regarding disclosure of information

Not applicable.

9.5 Intellectual property rights

When distributing this Certification Practice Statement, no information may be altered, removed, or added. It must be clearly stated that Expisoft AB is the issuer of this policy document.

9.6 Representations and warranties

9.6.1 CA's obligations and warranties

Described in the respective Certificate Policy.

9.6.2 RA's obligations and warranties

Described in the respective Certificate Policy.

9.6.3 Obligations and warranties of e-identification holders

Described in the respective Certificate Policy.

9.6.4 Obligations and warranties of the Relying party

Described in the respective Certificate Policy.

9.6.5 Obligations and warranties regarding other participants

Not applicable.

9.7 Disclaimers of warranties

Described in the respective Certificate Policy.

9.8 Limitations of liability

Described in the respective Certificate Policy.

9.9 Indemnities

Not applicable.

9.10 Term and termination for this Certification Practice Statement

9.10.1 Commencement of the period

This Certification Practice Statement shall be effective upon its publication on the Issuer's website.

9.10.2 Termination of the period

This Certification Practice Statement shall remain in force until it is replaced by a new version or until the CA ceases its operations.

9.11 Individual notices and communications with participants

The Issuer reserves the right, when necessary, to provide certain types of information about the CA service via e-mail or the Issuer's website, provided that this does not conflict with this Certification Practice Statement or the associated Certificate Policies.

9.12 Amendments of this Certification Practice Statement

See chapter 1.4.

9.13 Dispute resolution procedures

Any dispute arising from this Certification Practice Statement shall be finally settled by arbitration in accordance with the Rules for Expedited Arbitration of the Arbitration Institute of the Stockholm Chamber of Commerce. The place of arbitration shall be Stockholm, Sweden. The reference to arbitration shall not apply in consumer relationships.

9.14 Governing law

Swedish law shall apply to this Certification Practice Statement and to any legal relations arising therefrom.

9.15 Compliance with applicable law

The operation of the CA system shall be carried out in accordance with Swedish law.

9.16 Other provisions

Not applicable.

10 Definitions and abbreviations

The table below contains the terms, definitions, and abbreviations used in this Certification Practice Statement.

Approved by:	CEO, Christina Pettersson	Date:	2025-10-08

Term	Definition
Administrator	Trusted person at an agent who has been authorized by their organization to order and distribute e-identifications for their organization and the customers for whom they act as a representative.
Agent	An Agent is a reseller organization that has been authorized to order, manage, distribute, and revoke e-identifications for its own customers.
Agreement	The agreement between the Issuer and the Ordering organization for the issuance of an ordered e-identification.
Asymmetric cryptosystem	Cryptosystem where different keys are used for encryption and decryption.
Authentication	Verification/authentication of a stated identity (identification).
Authorized person	Physical person at the Ordering organization who is authorized to approve that the order is placed in the organization's name. For private Swedish companies, a signature by an authorized signatory is required. For foreign organizations, associations, municipalities, authorities, and state-owned companies where no authorized signatory exists or is publicly available, a signature by a person in a senior management position is required.
CA environment	CA environment includes CA systems with peripheral equipment, comprising both hardware and software.
CA service	The function of the Issuer responsible for issuing, managing, and revoking certificates and e-identifications.
CA policy	See Certificate Policy
Card	See Smart card.
CA-system	The isolated system in which the Issuer’s private key is securely stored and used, within dedicated hardware (HSM).
Catalog/X.500 catalog	A repository that contains issued certificates, associated public keys, and certificate revocation lists (CRLs).
Certificate	An electronic X.509 certificate, signed by the CA service, confirming the association of a public key with a specific individual or function within an organization.
Certificate Authority	Trusted organization providing a CA service whose task is to create and issue certificates (e-identifications).
Certificate chain	A certification path (certificate chain), i.e. an ordered sequence of certificates enabling the end-entity certificate to be validated starting from a trusted root key.
Certificate Policy (CP)	Regulations that the Issuer shall apply when issuing certificates.
Certificate Practice Statement (CPS)	A document produced by the Issuer that describes how the requirements stated in the Certificate Policy are fulfilled.
Certificate Revocation List (CRL)	A periodically updated, timestamped, and signed list issued by the CA, identifying certificates revoked prior to their expiry.
Certification Authority Administrator (CAA)	A role with overall responsibility for ensuring that the issuance and management of certificates comply with governing policies, and that our CA continues to be a trusted issuer.
Consignment	A consignment is something that is sent from one place to another.
Cross certificate	A certificate issued by one certification authority that binds another CA to its public key.
Cryptotext	Information produced from plain text through encryption with the purpose of making the content unreadable to unauthorized parties.
Customer	An organization/legal entity that purchases e-identification from the Issuer.
Customer data	The information about the Purchaser, Ordering organization/Customer that the Issuer needs to be able to issue the e-identification.
Delivery address	Address to which the ordered product should be delivered.
Digital signature	A digital signature is the electronic counterpart of a handwritten signature. It is generated by applying the signer’s private key to digital information through a defined procedure. A digital signature provides non-repudiation (assurance of origin) and integrity (verification that the information has not been modified after signing).

eid.expisoft.se	The Issuer's ordering service for e-identifications and certificates. Also referred to as the Issuer's ordering portal.
E-identification(s)	A collective term for the different certificates issued by the Issuer. An e-identification is a general term for one or more certificates containing information that enables the holder to identify themselves or sign something electronically.
E-identification holder	The organization or person within an organization listed as the holder of an issued certificate and who uses it.
Electronic ID (EID)	See e-identification
Electronic identification	See Authentication
Encryption	The transformation of plaintext into ciphertext using an encryption system and an encryption key, for the purpose of preventing unauthorized access (reading) of confidential information.
E-service	A digital service provided by a public authority or another organization. An e-identification is used to identify the individual accessing the service.
E-service identification (Card)	A personal e-identification consisting of two certificates: one certificate is used to authenticate the holder, and the other is used to enable the holder to digitally sign various documents. A personal e-identification is also referred to as an e-service identification when it is linked to a specific company or government agency and used in a professional context. The e-identification is used for electronic communication within an organization or with other organizations. The E-service identification Card is a smart card–based e-identification stored on an active card in PKCS#15 format. The plastic card containing the chip can be provided with a visual identity as a complement to the electronic identity. The e-identification is protected by a PIN.
E-service identification (File)	A personal e-identification consisting of two certificates: one certificate is used to authenticate the holder, and the other is used to enable the holder to digitally sign various documents. A personal e-identification is also referred to as an e-service identification when it is linked to a specific company or government agency and used in a professional context. The e-identification is used for electronic communication within an organization or with other organizations. The e-identification is used for electronic communication within an organization or for communication with other organizations. The E-service identification File is an e-identification that can be stored on the holder's computer or another device (e.g., smartphone) as a file in PKCS#12 format. The e-identification is protected by a password.
E-service provider	A public authority or other organization that provides a digital service.
File certificate	See Soft Certificates
General terms and conditions	These are the terms described in this document that apply to the ordering of e-identifications from Expisoft.
Hard Certificates	Certificate stored on smart cards and protected by a PIN. See E-service identification (Card).
Hardware Security Module (HSM)	A Hardware Security Module (HSM) is a physical device that protects and manages (asymmetric) cryptographic keys. Encryption keys can never be extracted from the HSM; they can only be used for encryption and signing of data sent to the device.
Identification	Process in which a user or resource states (presents/claims) its identity. After the identity has been provided, the authenticity of the identity is verified. (See authentication).
Information Systems Security Officer (ISSO)	Supervisory role responsible for the CA function.
Initial PIN	The PIN assigned by the Issuer during personalization of the active card.
Invoice address	Address to which the invoice should be sent.
Invoice reference	Reference that the customer wants included on the invoice. Often used to identify who/which function should bear the cost.
Issuer	See Certificate Authority
Key generation	The process during which public and private key pairs are generated.

Log	Continuously collected information about the operations performed in a system.
Non-repudiation	Principle meaning that the execution of a specific action cannot later be denied by the actor. Non-repudiation is achieved when the e-identification holder digitally signs the action.
Object identifier (OID)	A type within the ASN.1 (Abstract Syntax Notation One) standard, SS-ISO 8824 (§ 26), that provides a mechanism suitable for assigning unique names to objects, e.g., this policy. In Sweden, the Information Technology Standardization (ITS) body is responsible for registering unique OIDs.
Order number	A unique identifier for an order placed in our ordering portal.
Ordering organization	The legal entity placing the order, which may be the customer themselves or an agent/reseller for the customer.
Organization number	A unique number that identifies an organization in Sweden.
Period of use	The period during which a root certificate and its associated issuer keys can be used to generate e-identifications. The usage period can be defined as the validity period of the root certificate minus the validity period of the issued certificates. Example: If the root certificate has a validity of 12 years and the e-identifications have a validity of 2 years, then the usage period of the root certificate is 10 years.
Period of validity	The time span between two date-time values during which a certificate is considered valid and operational.
Personalization	The process of equipping the Smart card with the graphical and logical information required to link the cardholder to a specific card.
PIN	Personal Identification Number, a password usually consisting only of digits.
PIN letter	A letter linked to the ordered certificate that contains the codes needed to download/install, use, and revoke the e-identification.
Power of attorney	A document granting a person the authority to act on behalf of another.
Privacy protection	Protection against information being modified, either unauthorized or accidental, without detection.
Private key	A secret key (decryption key) in an asymmetric cryptosystem. Primarily used for generating digital signatures and for decrypting encrypted information.
Public key	A key that can be made public and is used for encryption in an asymmetric cryptosystem. It can also be used to verify the digital signatures of the public key holder.
Registration Authority (RA)	A role responsible for managing and issuing certificates in accordance with the company's certificate policy. Entrusted with registering and authenticating users and their personal data to ensure that correct certificates are issued.
Relying party	A party that trusts the information in a certificate for its decisions and e-services.
Requester	Physical person within the ordering organization who places the order for e-identification on behalf of their organization.
Reseller	See Agent
Revocation List	See Certificate Revocation List (CRL)
Root certificate	A certificate that attests that a specific public key belongs to a Certification Authority.
Security codes	Codes/passwords that the customer receives in a PIN letter upon delivery of the ordered e-identification.
Server identification	Also referred to as an Organizational identification. An organization-bound e-identification consisting of an authentication certificate. The certificate is based on the organization number and is used to authenticate the holder. The e-identification is stored on the organization's server as a file in PKCS#12 format and is protected by a password.
Service catalog	The Issuer's list of the e-services and e-service owners that trust the Issuer's certificates.
Service certificate	An electronic identification issued to an individual within an organization, used for internal or inter-organizational electronic communication.
Service provider	See E-service provider

Approved by:	CEO, Christina Pettersson	Date:	2025-10-08

Sign	To attach a digital signature to a message or a data set.
Smart card	A plastic card with a chip that can contain a personal e-identification with one or more certificates.
Smartcard	See Smart card.
Soft Certificates	Certificate stored (in PKCS#12 format) on media other than smart cards, for example locally on a PC or on a USB memory stick.
Stamp identification	An organization-bound e-identification consisting of a signing certificate; the certificate is based on the organization number and is used to sign various electronic documents on behalf of the organization. The stamp identification is stored on the organization's server as a file in PKCS#12 format. The stamp identification is protected by a password.
System Administrator (SA)	Role within IT with overall responsibility for the IT support of the CA function.
Unique identifier	Unique code/password used to make the PIN letter and/or private keys accessible only to the holder of an e-identification and to enable the holder to revoke the certificate.
Verification	The process of validation, primarily referring to verifying that a signature was generated by the entity indicated as the issuer of the signed information.
Website	https://eid.expisoft.se/ or another website that the Issuer provides to the ordering organization.