Certificate policy

E-service Identification Card

Versions			
Ver.no	Date	Name	Description
0.1	2025-09-24	CAA, Linda Fagerholm	English version created
1.0	2025-09-30	CEO, Christina Pettersson	Document approved

Roles and responsibilities of the document			
Author:	CAA, Linda Fagerholm	Date:	2025-09-24
Reviewed by:	Product owner CA, Katarina Eriksson	Date:	2025-09-29
Approved by:	CEO, Christina Pettersson	Date:	2025-09-30

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:	2025-09-30

Table of contents

1 Introduction

This document is a Certificate Policy (CP) that is owned and managed by Expisoft AB, hereinafter referred to as the “Issuer". This CP describes the technical and security requirements for the issuance, management, revocation, and renewal of the certificates covered by the policy (see chapter 1.1).

The Certificate Policy describes the certificates themselves and the requirements that the certificates must meet. A separate document, the Certification Practice Statement (CPS), describes the procedures and processes by which the Issuer fulfils the requirements set out in this Certificate Policy.

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

This policy 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.

Both the CP and CPS 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 policy outlines the requirements for issuing the following type of certificate:

- Personal e-identifications on card, also referred to as E-service Identification Card. A personal e-service identification can be considered the electronic equivalent of a physical company ID/organization ID that is, an identification that guarantees a person's affiliation with a specific company or organization, often as an employee.

1.2 Document name and identification

The certificates issued shall include object identifiers (OIDs) corresponding to this policy, certifying that the Issuer has issued and verified the certificates in accordance with the procedures established in this policy.

Name of the policy: Expisoft Certificate policy E-service Identification Card
(The Swedish name is Expisoft Certifikatpolicy E-tjänstelegitimation Kort)
Object identifier (OID): 1.2.752.54.9.2.25.X
This OID is found in the Certificate Policy (OID) attribute in the issued certificates.

The following certificates and CA instance are covered by this Certificate Policy:
OID: 1.2.752.54.9.2.25.3
Product name: e-Tjänstelegitimation Kort
CA instance: ExpiTrust e-Tjanstelegitimationer kort CA v4

1.3 PKI Parties and their responsibility

This chapter describes the parties affected by this Certificate Policy, as well as their commitments and responsibilities.

1.3.1 Issuer – Certification Authority (CA)

The CA is a trusted party among the involved parties that issues, signs, and delivers e-identifications and associated Certificate Revocation Lists (CRLs) to customers and relying parties in accordance with this policy. The Issuer (CA) may use services from third parties to carry out its tasks in accordance with this Certificate Policy (CP). It is the responsibility of the Issuer to ensure that any subcontractors comply with this policy as applicable.

1.3.1.1 Issuer's Commitments and Responsibilities

According to this policy, the Issuer undertakes to:

- Issue e-identifications in accordance with chapter 7.1.
- Provide the necessary control measures in accordance with chapters 3 and 8.
- Perform checks of ordered and delivered e-identifications before key initialization and personalization are carried out according to chapter 6.1.
- Ensure that e-identifications are stored and delivered to the Requester in accordance with chapter 6.1.2.
- Ensure that the e-identification holder receives the necessary information to enable the download of certificate files.
- Provide a revocation service in accordance with chapter 4.9.
- Implement security measures in accordance with chapter 6 of this policy.
- Protect the CA service's private key as specified in chapter 6.2.
- Ensure that the CA service's private key *can only be used* to sign e-identifications/certificates, revocation lists, logs, or other functions described in this policy.
- Take responsibility for services carried out by the Registration Authority (RA) on behalf of the Issuer.
- Establish, publish, and maintain a current Certification Practice Statement (CPS).
- Review that the policy is consistent with the CPS, correct any discrepancies, and publish updated versions of the documents.

The Issuer shall also provide a support function that assists customers and e-identification holders regarding certificate issuance, maintenance, or revocation.

By issuing and signing certificates that contain object identifiers referring to this policy, the Issuer certifies that it has verified the information in the e-identification in accordance with the procedures established in this policy. However, the Issuer is not liable for damages resulting from incorrect information in an e-identification or revocation list unless the Issuer has been found to be grossly negligent,

1.3.2 Registration Authority (RA)

The Registration Authority (RA) is appointed by the Issuer and shall operate in accordance with this policy and follow the practices described in the Certification Practice Statement (CPS). The RA function and its personnel are responsible for the identification and verification of e-identification holders and proxy holders. The Issuer is responsible for the services performed by the RA on behalf of the Issuer, such as the issuance and revocation of e-identifications/certificates.

1.3.2.1 Commitments and Responsibilities of the RA Function

According to this policy, the RA undertakes to:

- Carry out the actions described in chapter 3 with the aim of ensuring that the information forming the basis for the e-identification to be issued is accurate.
- Ensure that activation data for issued e-identifications are archived with the RA in accordance with chapter 2 of this policy.
- Protect the private key in accordance with this policy, the associated Certification Practice Statement (CPS), and its agreement with the Issuer.
- Undergo internal certification process testing through random sampling to maintain high standards.

1.3.3 Resellers of the issuer's e-Identification products

1.3.3.1 Reseller Commitments and Responsibilities

According to this policy, the Reseller undertakes to:

- Carry out the actions described in chapter 3 with the purpose of ensuring that the information forming the basis for the e-identification to be issued is accurate.
- Comply with the agreement established between the Issuer and the Reseller, which governs the responsibilities and obligations towards both the Issuer and the customers for whom the Reseller is responsible.
- Log in to the Issuer's web portal and, via the order portal, order or revoke e-identifications on behalf of its customers.

1.3.4 Requester within a customer organization

1.3.4.1 Commitments and Responsibilities of the Requester

According to this policy, the Requester undertakes to:

- Carry out the actions described in chapter 3 with the purpose of ensuring that the information forming the basis for the e-identification to be issued is accurate.
- Comply with the agreement established between the Issuer and the Requester, which governs the responsibilities and obligations towards the Issuer and the organization for which the Requester is responsible.
- Log in to the Issuer's web portal and, via the order portal, order or revoke e-identifications on behalf of their organization.
- Provide truthful information in the e-identification application.

- If the application is sent directly to the Issuer's RA function and not via an Agent, ensure that the power of attorney for the order, signed by an authorized person, submitted in original paper form by mail to the Issuer's RA function. Alternatively, the authorization may be signed digitally by an authorized person using Swedish Mobile BankID.

1.3.5 Holder of e-identification

E-service identification Cards are held by individuals.

1.3.5.1 Obligations and liabilities of the e-identification holder

The e-identification holder undertakes according to this policy to:

- When applying for an e-identification, commit to following the applicable procedures described in chapters 3 and 4 of this policy.
- The e-identification holder shall ensure that they maintain control over their e-identification and prevent unauthorized use of the credential by:
    - not storing the PIN or password together with the e-identification and not revealing it to unauthorized people.
    - protecting the e-identification in the same way as valuables.
    - never leaving an activated e-identification unprotected.
- The e-identification holder shall immediately notify their organization to have the e-identification revoked if there is reason to do so according to the general terms and conditions for ordering Expisoft e-identifications (available at www.expisoft.se) or if any of the following occur:
    - If any information in the e-identification is deemed incorrect, or if any details or conditions of the e-identification have changed since issuance, e.g., first or last name.
    - If the private key associated with the e-identification has been compromised or there is reason to suspect it has been compromised.
      Example: There is suspicion that the password to a user's certificate file has been compromised.

Note: The issuer may also, on its own initiative, revoke an e-identification if the e-identification holder is found not to fulfil their obligations, or if there is suspicion that the e-identification has been compromised or disclosed.

1.3.6 Obligations and liabilities of the Relying party

A Relying party is an organization that offers an e-service where e-identifications are used for identification and authentication and/or electronic signature. The Relying party is an organization that relies on the chain between the issuer of electronic identities, the user, and eventual certificate issuer to be correct. It is the Relying party's responsibility to verify the authenticity and applicability of the e-identification, as well as its validity in accordance with chapter 4.9, revocation and suspension of e-identifications.

An example of a Relying party could be a government agency that has implemented identification and signature in an e-service provided by the agency and may choose either to perform this verification itself or to use a subcontractor to carry out this function.

1.4 Certificate (e-identification) usage

It is the Relying party or their organization that decides for which purposes the issued e-identifications can be used. Suitable uses include, for example:

- Identification of websites, e-services, and secure SSL communication between individuals, authorities, and companies.
- Electronic stamps for digital approval of documents, records, etc.
- Identification (authentication) when accessing services and providing information.
- Privacy protection (encryption) of communication or data stored on various media.
- Electronic signature for digital signing of documents, records, emails, etc.

It is the Relying party's decision that determines which applications/e-services the issued e-identifications according to this policy shall be used for. To guide this decision, the Relying party has, in addition to any internal regulations, this policy and the associated Certification Practice Statement (CPS).

1.5 Policy administration

1.5.1 Organization responsible for administering this policy

The issuer Expisoft AB is responsible for the management, administration, and maintenance of this CP. Questions regarding this CP 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 CPS suitability based on CP

The role of Certificate Authority Administrator (CAA) (see 5.2.1) is responsible for the suitability and applicability of this CP in the associated Certification Practice Statement (CPS).

1.5.4 Approval procedure for this Certificate Policy (CP)

The role of Certificate Authority Administrator (CAA) (see 5.2.1) is responsible for the approval process of this document. Any changes made must be documented in the form of an updated CP, which is to be published on the Issuer's website.

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 CP, and the associated CPS shall be published on the Issuer's website.

2.2 Publication of certificate-related information

The issuer shall provide the following information:

- This policy and the associated Certification Practice Statement (CPS).
- Certificate Revocation Lists (CRLs).
- All issued root certificates.
- Contract templates, power of attorneys and terms for Agents.
- General terms and conditions for ordering e-identifications.

Certificate Revocation Lists and root certificates shall always be available through the issuer's website.

2.3 Times and frequencies of publication

For the timing and frequency of the publication of revocation lists, see 4.9.7.

2.4 Authorization control for storage locations

Only personnel trusted by the CA service shall have the ability to publish and update the information on the relevant websites. No authorization control is required to retrieve and read the information according to chapter 2.2 above.

3 Identification and authentication (I&A)

This chapter describes the rules that apply to the identification and authentication of physical individuals and organizations involved in the process of verifying and issuing certificates. Personal data must be handled in accordance with the Swedish Data Protection Act and General Data Protection Regulation, or other applicable laws/agreements that provide a legal basis for processing the personal data.

Each issued certificate contains a number of fields that can be linked to the organization and the e-identification holder to whom the certificate applies (see chapter 3.1).

3.1 Naming

3.1.1 Types of names

The following information is mandatory:

Information	Content requirements
Name	The name of the organization registered with the Swedish Companies Registration Office (Bolagsverket) or the Swedish Tax Agency (Skatteverket).
Organization number and serial number	Organization number registered with the Swedish Companies Registration Office (Bolagsverket) or the Swedish Tax Agency (Skatteverket), along with a serial number.
Unique identifier for e-identification	Unique identifier (64-bit), used to distinguish e-identifications and their certificates.
Common Name (CN)	This field shall contain the name of the holder, an optional title field, and the name of the organization.

Certificates may also contain other types of information (see chapter 7.1).

3.1.2 Need for meaningful names

The names in the certificates (see 3.1.1) shall be meaningful in the sense that the Issuer can establish the connection between these names and the e-identification holder.

3.1.3 Anonymous or pseudonymous e-identification holders

E-identifications must identify the e-identification holder through correct names; anonymity or pseudonyms are not allowed.

3.1.4 Rules for interpreting different name formats

Most special characters are not handled/allowed. Such characters will be corrected.

3.1.5 Unique names

The mandatory information according to 3.1.1 shall uniquely identify the e-identification holder. Only officially registered identity information is accepted. If the organization is officially registered, the registered name should be used. In Sweden, the name registered with the Swedish Patent and Registration Office (PRV) or equivalent shall be used. Although not recommended, it is possible for the same e-identification holder (organization) to have multiple certificates with the same identity in the subject field. The certificates can then be distinguished by the certificate serial number (not to be confused with the serial number in the subject field).

3.1.6 Recognition, authentication, and the role of trademarks

It is the responsibility of the e-identification holder to ensure that the choice of name in the certificate's subject field does not violate any trademark or trademark rights.

3.2 Initial identity validation

3.2.1 Method to prove possession of the private key

Since the Issuer generates the key pair, the Requester does not possess any private key before the certificate is delivered to them.

3.2.1.1 E-service Identification Card (personal)

Depending on the type of smart card, the private and public key may already be stored on the smart card when it arrives at the CA service's RA function or an Agent. Alternatively, the keys are generated on the card by the CA service. The private key exists only on the smart card. After validation of the card's key pair, the CA service issues a certificate to the Requester. The Requester does not have access to any private key before receiving the e-identification.

3.2.2 Authentication of the organization's identity

The organization's identity, in the form of name details in the certificate's subject field, must be verified and checked along with the organization number. Abbreviations and/or various suffixes to the stated company/organization name are permitted, provided that the name can be associated with the organization. The information in the order must be verified and signed by an authorized person before the order is submitted to the Issuer. For private Swedish companies, the signature of an authorized signatory is required. For foreign organizations, associations, municipalities, authorities, and state-owned companies where an authorized signatory does not exist or is not publicly available information, the signature of a person in a senior management position is required.

3.2.3 Authentication of the individual's identity

It is the Requester within the requesting organization (or Agent) to take the necessary actions to ensure that the information regarding the resource, function, or individual within the organization/company, on which the requested e-identification is based, is accurate. All orders must be signed by an authorized person (see chapter 3.2.2 for the definition of an authorized person). If the Requester is authorized, they may sign the order themselves.

3.2.4 Unverified data about the e-identification holder

Not applicable.

3.2.5 Validation of authorization of Agent

In cases where the Customer uses an Agent for ordering e-identifications, i.e. a Reseller, the relationship between the parties shall be governed by a separate agreement referring to this CP. Validation of the Agent's authorization shall be carried out by issuing a personal e-identification to the Agent's administrator. The Administrators e-identification shall be ordered and produced according to the procedure described in chapter 3.2.3. This e-identification shall thereafter be used to identify the Administrator when ordering new e-identifications for its own organization or its customers.

3.2.6 Criteria for collaboration

Not applicable. The certificates covered by this policy do not involve any interaction with other Certificate Authorities or PKIs.

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

Revocation of an e-identification may be initiated either by the e-identification holder, by one of the Customer's Agents, or by the Issuer itself. The e-identification holder shall be identified using the unique identifier that was distributed together with the e-identification in a PIN letter. Agents' Administrators shall identify themselves using their e-identification by logging in to a web portal provided by the CA service. Revocation may also be requested by contacting the Issuer's support function, in which case identification of the e-identification holder must be carried out. Revocation requests are handled in accordance with chapter 4.9.

4 Certificate life-cycle operational requirements

This chapter describes the operational requirements applicable to the Issuer, the RA function, the Requester, and the e-identification holder. The requirements cover application, issuance, revocation, archiving, and logging.

4.1 Order of e-identifications

4.1.1 Who can order an e-identification

A Customer apply for/order an e-identification through the Issuer's web portal. An Agent (Reseller for the Certification Authority) may order e-identifications on behalf of its respective customer or customer group.

4.1.2 Order procedure and responsibility

The Requester shall identify itself in accordance with chapter 3.1, and:

1. Complete the application documents and accept all terms and conditions.
2. An authorized person within the Requester's organization must sign the application document. For private Swedish companies, a company signatory is required. For foreign organizations, associations, municipalities, authorities, and state-owned companies where signatory information does not exist or is not publicly available, a person in a senior management position is required. This can either be done digitally using Swedish Mobile BankID or by printing and signing the order application on paper. The signature thereby certifies that:
    - The Requester is entitled to place the order for the e-identification.
    - The information provided in the application document is correct.

3. If the order application is signed on paper, the Requester must send the original signed application by post to the Issuer's RA function. The RA function receives and archives all application documents in accordance with chapter 4.3 and thereafter issues the e-identification.

If errors in an order cannot be resolved in consultation with the Requester, the Issuer reserves the right to reject the order.

The responsibilities of the Issuer and the e-identification holder are described in chapter 1.3.1.1 and 1.3.5.1.

The ordering process may vary between customer groups but must, from a security perspective, meet the requirements set forth in this policy regarding identification and authentication of the Requester in accordance with chapter 3. The responsibilities of the Agent are described in chapter 1.3.3.1.

4.2 E-identification order processing

The registration and management of the data required for issuing an e-identification shall be carried out in such a way as to prevent any mix-up of identity data, certificate files, and keys.

4.2.1 Identification and authentication

Identification and authentication of the Requester shall be carried out in accordance with chapter 3.1 of this policy. Each order for an e-identification through the Issuer's RA function or via an Agent shall be signed in order to be individually traceable to the person who requested the issuance of the e-identification.

4.2.2 Approval or rejection of an e-identification order

The Issuer's RA function may only approve the order and proceed with issuing an e-identification to the Requester if both of the following conditions are met:

- The Requester has fulfilled its obligations in accordance with chapter 1.3.5.1.
- The Issuer's RA Function has verified the Requester's information in accordance with chapter 3.1 of this policy.

All other orders for e-identification shall be rejected. A Requester whose order is rejected shall be informed of what is required for the order to be approved.

4.2.3 Processing time for certificate and e-identification request

The Issuer RA function shall issue and deliver e-identifications within the delivery time specified at the time of ordering, counted from the receipt of a signed and correct order. The Issuer's RA function shall also have the capability to handle express orders.

4.3 Certificate issuance

4.3.1 Activities during certificate issuance

Described in the Certification Practice Statement (CPS).

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

The Requester shall be informed in writing (for example by e-mail) by the Issuer's RA function that the ordered e-identification has been issued.

4.4 E-identification/ certificate acceptance

4.4.1 Procedures that establish acceptance of issued e-identification

By placing an order, the Requester accepts the terms and conditions in force at the time for the issuance of an e-identification in accordance with chapter 4.1.
The application itself shall be considered an acceptance of the intended certificate by the Requester and the authorized person who has signed the order.

The issuance of an e-identification confirms the Issuer's acceptance of the application as well as the information provided by the Requester in the application.

The e-identification holder accepts the issued e-identification (certificate) when identifying themselves and acknowledging receipt of the PIN letter, either as a registered letter by mail or digitally via authenticated access to the web portal.

4.4.2 Publication of issued e-identification by the certificate issuer

Once an e-identification has been issued, it shall be published on the Issuer's web portal, where the Requester can download their ordered certificate.

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

Not applicable. No parties other than the Issuer, the Requester, and, where applicable, an Agent needs to be notified when issuing e-identifications.

4.5 Key pair and certificate usage

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

The e-identification holder may only use the certificate and associated private keys of the e-identification for the purposes specified in this policy, see chapter 1.4.
Certificate usage must comply with the KeyUsage fields included in the certificate, see chapter 6.1.7. The e-identification holder shall also protect their private keys from unauthorized use and discontinue the use of the e-identification and its certificates when the e-identification has expired or has been revoked.

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

Before a Relying party (e-service provider) uses and accepts an issued e-identification and its associated certificate, the Relying party shall:

- Verify that the e-identification is suitable for the intended use.
- Verify the validity of the e-identification, i.e. that the certificate's signature is correct.
- Verify that the certificate's validity period (from and to dates) is correct.
- Verify that the certificate has not been revoked, i.e. that it does not appear on the most recently available Certificate Revocation List (CRL) from the Certification Authority service and/or check through an OCSP request that the certificate has not been revoked.

If the status of the e-identification cannot be verified at the time of use, for example due to a system or communication problem, it is up to the Relying party to decide whether to accept and use the certificate.

4.6 E-identification renewal

Not applicable. Renewal of an e-identification or its certificate is treated in this CP as a new order (see chapters 4.1 and 4.3).

4.6.1 Reasons for renewal of the e-identification

Not applicable.

4.6.2 Who can request renewal

Not applicable.

4.6.3 Handling of requests for renewal of the e-identification

Not applicable.

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

Not applicable.

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

Not applicable.

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

Not applicable.

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

Not applicable.

4.7 Renewal of the certificate key pair

When the Issuer generates the key pairs, new encryption keys are always created upon the issuance of a certificate. A renewal of a certificate's key pair is treated as a new order (see chapters 4.1 and 4.3).

4.7.1 Reasons for renewal of the certificate keys

Technical problems during the installation of a certificate may result in a request to renew a specific key pair.

4.7.2 Who can request a renewal of the certificate keys

Only the e-identification holder may request the renewal of a key pair, see chapter 4.1.1.

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

According to chapter 4.2.

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

According to chapter 4.3.2.

4.7.5 Procedures establishing acceptance of the certificate

According to chapter 4.4.1.

4.7.6 The Issuer's publication of certificates with new keys

According to chapter 4.4.2.

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

According to chapter 4.4.3.

4.8 Certificate modification

According to chapter 4.7.

4.8.1 Reasons for modifications of a certificate

According to chapter 4.7.1.

4.8.2 Who can request modification of a certificate

According to chapter 4.7.2.

4.8.3 Handling of requests for modification of a certificate

According to chapter 4.7.3.

4.8.4 Notification to the Requester regarding modification of a certificate

According to chapter 4.7.4.

4.8.5 Procedures that establish the acceptance of a modified certificate

According to chapter 4.7.5.

4.8.6 The Issuer's publication of the modified certificate

According to chapter 4.7.6.

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

According to chapter 4.7.7.

4.9 Certificate revocation and suspension

Revocation of an e-identification means that all certificates associated with the e-identification are revoked. The Issuer shall provide a web service for revoking e-identifications, which also ensures the availability of information about revoked e-identifications throughout the lifetime of the e-identification. Certificate Revocation Lists (CRLs) shall be published regularly to a public service so that revocation checks can be performed when using the e-identification.

4.9.1 Reason for certificate revocation

An e-identification shall be revoked if:

a) A revocation request is received from the e-identification holder, their organization, or an Agent.

b) Any information in the e-identification is, or is suspected to be, incorrect.

c) The private key or associated codes linked to the e-identification have been disclosed, or there is suspicion that they have been compromised.

d) The e-identification holder has lost their e-identification, i.e. the smart card.

e) Any of the information or attributes contained in the e-identification, such as name, has changed.

f) The certificate has become redundant (for example, a duplicate certificate has been issued).

g) Any other reason exists that renders the e-identification obsolete or threatens its encryption keys.

h) The e-identification holder's agreement with the Issuer is terminated.

i) The Issuer has essential reasons to replace the current policy with a new version containing security-relevant changes.

j) The private key of the CA service is suspected to be compromised.

k) The certificate delivered has not been paid for after two reminders have been sent.

The Issuer may, on its own initiative, revoke an e-identification if the e-identification holder fails to fulfil their obligations under this policy or violates applicable law.

4.9.2 Who can request a revocation

Revocation of e-identifications may be requested by the e-identification holder or their Agent. For the e-identifications covered by this policy, the PIN letter contains a unique identifier that the holder may use if they wish to revoke the e-identification.

The Issuer may also, on its own initiative, revoke an e-identification/certificate if unauthorized use of the e-identification is suspected. Other possibilities for revocation are governed by separate agreements with the respective contracting party.

4.9.3 Procedure for revocation request

Described in the Certification Practice Statement (CPS).

4.9.4 Processing time for revocation requests

A revocation request made through the Issuer's website or manually via the Issuer's support function, during support hours, shall be executed without delay, and a new revocation list shall be published after the revocation request has been processed. The decision to revoke shall be made directly in connection with the revocation request, after verification of the identity of the requester. An incoming revocation request via the Issuer's website during a scheduled maintenance window/outage shall in such cases be handled after the planned interruption. Operational notices are published on the ordering portal in advance of scheduled outages.

4.9.5 Time within which the CA must process revocation requests

A revocation request shall be handled within one business hour from the time the request is received.

Example: When the e-identification holder revokes a certificate directly via the Issuer's website, the revocation process is initiated immediately. However, if a written revocation request is received by the Issuer on a public holiday, it shall be processed during the first business hour of the following working day.

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

It is the responsibility of the Relying party, either directly or through an outsourced function, to check whether an e-identification has been revoked. The check shall be performed as follows:

- A Relying party retrieving a revocation list from a repository shall ensure its authenticity by verifying its digital signature and certification chain.
- The Relying party shall also verify the validity period of the revocation list to ensure it is up to date.
- In cases where the Relying party's validation function supports OCSP, the validity of an e-identification and its certificate may also be checked using this protocol.
- If a certificate has been revoked, the e-identification shall not be accepted.
- If a revocation check as described above cannot be performed (for example due to operational disturbances), the e-identification should not be accepted; however, the Relying party may choose, at its own risk, to accept the e-identification in such cases.

4.9.7 Frequency of publication of revocation lists (CRL)

New Certificate Revocation Lists (CRLs) shall be published every hour, around the clock, and have a validity period of 24 hours, i.e. the nextUpdate attribute shall be set to 24 hours.

4.9.8 Maximum delay of publication of revocation lists (CRL)

The delay from the generation of a new Certificate Revocation List (CRL) until it is available for revocation checking of issued certificates (available via CDP/OCSP) shall not exceed 10 minutes.

4.9.9 Online revocation request and status/revocation check

For the certificates covered by this policy, online revocation requests and status/revocation checking of an e-identification via the OCSP protocol shall also be offered to Relying parties as a complement to Certificate Revocation Lists (CRLs).

4.10 Certificate status services

4.10.1 Properties

Revocation lists shall be published in the Issuer's public repository/directory in accordance with the criteria and intervals described in chapter 4.9. An OCSP service shall be made available to users of the e-identifications.

4.10.2 Availability

Both the CRL and OCSP services shall be available 24 hours a day, 365 days a year (24/7/365), with exceptions only for brief unscheduled outages or planned maintenance.

4.11 End of e-identification subscription

If an issued e-identification is no longer needed, the e-identification holder shall revoke it.

4.12 Key escrow and recovery

Not applicable. Key escrow and key recovery are not supported.

5 Facility, management, and operational controls

This chapter describes the physical, procedural, and personnel controls implemented by the Issuer and its RA function.

5.1 Physical security controls

Physical security is intended to protect the Issuer's premises, equipment, and information assets. The CA system shall be safeguarded against accidents, technical system failures, human error or negligence, and criminal acts. The objective of physical security is to prevent unauthorized physical access, damage, and operational disruptions of the CA system.

5.1.1 Physical location and structure

The CA system shall be physically located in a secure data center. The room housing the CA system shall be an "interior" room, i.e., without walls adjoining an exterior facade or any windows. Walls, ceiling, and floor shall be solid. The room shall be locked, and access shall be granted only to authorized personnel. The room should be equipped with an entry control system consisting of a card reader and keypad. All authorized personnel shall be issued a personal access card with their own PIN. Within this room, the CA system shall additionally be stored in a locked cage secured with two physical padlocks. This room is referred to in this policy as the CA system's operating environment.

5.1.2 Physical access

The CA system shall be protected against unauthorized access. Access control shall be used to regulate entry to the CA system's operating environment. A logbook shall be maintained of all individuals granted access to this area. Access to the CA system further requires the presence of multiple people (see chapter 5.2.2). In the event of a critical incident where it is not possible to assemble two authorized persons simultaneously, an exception to the dual-control requirement may be made; however, such exceptions must be thoroughly documented. The area shall also be equipped with the necessary alarms to ensure detection of any type of unauthorized intrusion. The private keys used for signing certificates and revocation requests shall be physically protected within an HSM module, ensuring they cannot be exposed even in the event of a physical breach of the facility.

5.1.3 Power supply and cooling

To ensure uninterrupted 24/7/365 operation of the CA function's power supply and cooling, the system shall be capable of withstanding a power outage of up to 24 hours.

This capability shall be tested at least once per year.

5.1.4 Water exposure

The CA system shall be protected against water exposure. Water detection alarms shall be in place.

5.1.5 Fire protection

The CA system shall be protected against fire. Fire alarms shall be in place.

5.1.6 Storage of media

The Issuer shall ensure that archives, backups, and distribution media are stored in a manner that prevents loss, tampering, or unauthorized use of stored information. The handling of personal data shall comply with applicable legislation in this area, including the Swedish Personal Data Act, the Data Protection Directive, and the General Data Protection Regulation (GDPR).

5.1.7 Waste management

Sensitive material shall be destroyed in a secure manner to ensure that it cannot fall into the possession of unauthorized parties.

5.1.8 Backup at another location

Archives and backups shall be stored separately from the central CA system. The copies shall be stored in such a way that the information is protected against theft, alteration, destruction, or unauthorized use.

5.2 Procedural controls of the CA function

The Issuer is responsible for the administration and procedures for issuing e-identifications and revocation lists. Procedures ensuring traceability shall be in place so that misuse and errors at any stage of the process can be detected and corrected.

5.2.1 Trusted roles

The following roles shall exist within the CA function for the issuance of e-identifications:

1. Information Systems Security Officer (ISSO) – These individuals hold ultimate responsibility for the security of the CA system and shall be present during particularly security-critical operations.

2. Certification Authority Administrator (CAA) – Responsible for central operations in the CA system. The CAA is accountable for establishing new CAs, assigning RA and SA privileges, reviewing logs, and ensuring compliance with the CP and CPS.

3. System Administrator (SA) – Responsible for operations. The SA performs installations, system maintenance, and replacement of backup media. This person must be approved by the CAA to work with the CA service, but particularly security-sensitive tasks must be carried out under the supervision of the CAA or ISSO.

4. RA Administrator – Manages certificate order requests and issues or revokes certificates.

5. Trusted Person – An individual trusted by the CA service who may assist in activities requiring at least two people but not a specific role. Trusted persons are appointed by one of the CEO, COO, or CAA.

Additionally, there is a customer role, Administrator, who acts as an agent for their organization and is authorized to request, distribute, and revoke e-identifications on behalf of their organization.

Beyond the above roles tied to the CA function, there is also an independent role, Auditor, tasked with reviewing the work of CA personnel at specifically agreed intervals (see chapter 8).

5.2.2 Requirements for number of people per task

Certain sensitive tasks and operations require the presence of more than one person. This policy prescribes several such instances, namely:

- Issuance of certificates requires the participation of at least two trusted people, of whom at least one must hold the RA role.
- Generation of new Issuer keys and a new root certificate requires the presence of at least two different individuals. Both the ISSO and CAA roles must be present (see chapter 6.2.2).
- Log handling of the central CA system requires the presence of two people. One individual must hold the ISSO role, and the other must hold one of the following roles: ISSO, CAA, SA, or Trusted Person.
- Physical access to the secured backup of the CA's private key requires the presence of at least two different individuals. Both the ISSO and CAA roles must be present.
- Physical access to the central CA system requires at least two different individuals, one of whom must hold either the ISSO or CAA role, and the other must hold one of the following roles: ISSO, CAA, SA, or Trusted Person.

In the event of critical incidents affecting operations and availability, where it is not possible to assemble two authorized persons simultaneously, exceptions to the two-person requirement may be made. Such exceptions must, however, be thoroughly documented for follow-up and security review.

5.2.3 Identification and authentication for each role

Identification and authentication for each role described in chapter 5.2.1 shall be performed in a secure manner, meaning that strong authentication shall be used whenever these users carry out tasks involving the CA function.

5.2.4 Roles that require task separation

An individual serving in the Auditor role may not simultaneously hold any of the roles associated with the CA function as defined in chapter 5.2.1.

Both internal and external Auditors may be engaged; the essential requirement is that the individual is independent. However, the person must be familiar with the CA service's operations, procedures, administrative roles, as well as this CP and the accompanying CPS in order to perform their duties effectively.

5.3 Personnel controls

5.3.1 Requirements for competence, experience and formal qualifications

Personnel holding roles considered critical from a security perspective shall be specifically selected, reliable individuals who have demonstrated suitability for such positions. Personnel may not have any other duties that could conflict with the obligations and responsibilities associated with their roles within the CA system.

5.3.2 Background check

Employee background checks shall be conducted by the Issuer and shall include verification of previous employment as well as personal background screening.

5.3.3 Training requirements

All personnel of the Issuer involved with the CA system shall be provided with the necessary training and knowledge to perform their duties correctly.

5.3.4 Requirements for competence development

All personnel shall be provided with the necessary skills development whenever systems or procedures are changed.

5.3.5 Job rotation

Not applicable. Job rotation is not required for the certificates covered by this policy.

5.3.6 Disciplinary actions for unauthorized activities

Measures shall be taken in the event of unauthorized activities.

5.3.7 Requirements for supplier independence

Suppliers and subcontractors to the CA service shall not undertake any other duties that conflict with the obligations and responsibilities arising from their assignments to the CA service.

5.3.8 Documentation for personnel

Personnel shall be provided with sufficient instructions to correctly perform their duties within the CA system.

5.4 Audit logging procedures

5.4.1 Types of events to be recorded

The following events (at a minimum) shall be logged in the CA system:

- Creation of user accounts for CA/RA administrators (security log).

- Initiation of transactions such as issuing or revoking e-identifications, including information on who requested the transaction, the time, the type of transaction initiated, and the outcome of the requested transaction (security log).
- Order documentation, including the signature of an authorized person, validation of orders, and identification of the person who approved the order (security log).
- Installation and updating of software (operations log).
- Relevant information regarding backups (date, time, etc.) (operations log).
- System startup and shutdown (operations log).
- Date and time of hardware upgrades (operations log).
- Date and time of operations log clearance (operations log).

5.4.2 Frequency of log analysis

The logs shall be reviewed and analyzed at regular intervals in order to detect undesirable events.

5.4.3 Retention period for logs

Security logs shall be retained for at least 10 years as part of the archived information. Operational logs are not required to be retained for the same duration (no specific retention period applies).

5.4.4 Protection of logs

Logs shall be protected against unauthorized modification and be provided with individual timestamps.

5.4.5 Backup of logs

Backups of logs shall be created to ensure that the logs are preserved even in the event of a system crash or if a person with malicious intent deliberately deletes logs in the CA system.

5.4.6 Log collection system

There is no requirement for a centralized log collection system, provided that logging is performed for all events listed in chapter 5.4.1.

5.4.7 Notification to the originator of the log event

For security reasons, no message shall be displayed indicating that a log entry has been created.

5.4.8 Vulnerability assessment

A risk and vulnerability analysis of the CA operations shall be carried out at least once per year.

5.5 Records archival

5.5.1 Type of information to be archived

The following information (at a minimum) shall be archived:

- Transactions containing certificate issuance or revocation requests signed by an authorized person, including the content of the e-identification.
- Received revocation requests for issued certificates in accordance with chapter 4.9.1.
- Order documentation, including the signature of the authorized person, validation of orders, and information on who approved the order.
- History of previously used issuer keys.
- Agreements related to e-identifications.
- Audit reports in accordance with chapter 8.
- Current and previously issued versions of this CP and the corresponding CPS.
- Issued CA certificates (including root certificates).
- Security logs

5.5.2 Retention period for archives

Archived information in accordance with chapter 5.5.1 shall be retained for the lifetime of the information, plus three years. For a root key with a validity period of 12 years, this means an archival period of at least 15 years.

5.5.3 Protection of archives

Archived information shall be protected against unauthorized alteration and loss and shall only be accessible to authorized personnel. Information regarding individual events may be made available upon request by the involved party, a representative of the involved party, or another authorized individual. Archived material classified as confidential shall not be accessible to external parties in its entirety, except where required by law or by a court order.

5.5.4 Backup of archives

Not applicable.

5.5.5 Requirements for timestamping of archived documents

The time of archiving shall be recorded.

5.6 CA key changeover

At least three months before the validity period of a valid root certificate expires, new CA keys (issuer keys) and a new self-signed root certificate must be generated. During a transition period, both the old and the new CA certificate shall be active simultaneously. Example: If the e-identifications that are issued have a validity period of two years, a new root certificate must be generated at least two years and three months before the old root certificate expires.

5.7 Compromise and disaster recovery

5.7.1 Procedures for major incidents

If an attempt at an intrusion or any other form of possible compromise of a CA becomes known, it shall be investigated immediately to determine the nature and extent of the damage. The scope of potential damage shall be assessed based on this, for example, whether the CA certificate needs to be revoked or not.

5.7.2 Damage to computers, software, and/or data

The Issuer shall regularly create backups of systems and information enabling restoration of the CA system and operations in the event of damage to software, computers, or other equipment. In the event of suspicion that the CA service's private key has been compromised, a risk analysis and investigation shall be conducted without delay to assess the extent of the damage and appropriate measures. If the investigation shows that it is likely that the key has been compromised, an assessment shall be carried out in accordance with chapter 5.7.1. If the decision is made that the CA service's operations must cease, actions pursuant to chapter 5.8 shall be implemented immediately and without delay, i.e., without consideration of the six-month notice requirement.
If the decision is made that the CA service may continue its operations, the Issuer shall take the following actions:

- Issue a new root CA certificate and transition to this certificate for certificate issuance, revocation lists, and OCSP service.
- Inform and distribute the new root CA certificate to all relying parties, Agents, and other relevant stakeholders.
- Revoke all e-identifications issued under the old Issuer key and publish a final revocation list.
- Cease issuance and publication of revocation lists (CRLs) and OCSP services under the old Issuer key, ensuring that relying parties performing revocation checks no longer trust previously issued e-identifications.
- Contact e-identification holders whose credentials were issued under the old key and offer them replacement with a new e-identification.

5.7.3 Disaster recovery and business continuity capability

The CA service shall maintain a business continuity plan (disaster recovery plan) describing the measures to be taken in the event of a disaster. This plan shall be executed in the event of any form of disaster, including suspected compromise of the CA service's private key. The plan shall be reviewed and updated at least annually to ensure its continued relevance.

5.8 CA termination

The termination of the Issuer's operations refers to a situation where all services associated with the Issuer are discontinued. Before the Issuer ceases its operations, the following measures shall be undertaken at a minimum:

- Inform all relying parties, Customers, Agents, e-identification holders, and other parties with which the Issuer has a relationship with. This should be done at least six months prior to the termination of operations.
- Terminate agreements with any Agents and subcontractors.

- Publicly announce the termination of operations to the market.
- Cease the issuance of new certificates.
- Ensure that all archives and logs are preserved in a secure manner for the agreed retention period.

6 Technical security controls

This chapter contains rules for the generation and installation of key pairs, the protection of keys, and other technical security controls.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The input to all key generation processes shall be a random number created in such a way and of such length that it is computationally infeasible to reproduce it, even with knowledge of when and in which equipment it was generated. The key generation process shall be designed so that no information about the private key is handled outside the key generation system other than through secure transfer to the intended location. Public keys shall be handled in such a way that their integrity is ensured.

6.1.1.1 Issuer Keys for signing certificates and revocation lists

Issuer keys used for the signing of certificates and certificate revocation lists (CRLs) shall be generated and operated within a physically secured environment in accordance with chapter 5.1. Access to this environment shall require the concurrent presence of at least two authorized persons, as specified in chapter 5.2.2. CA keys shall be generated within a Hardware Security Module (HSM) that is dedicated to the storage and use of cryptographic keys. The generation of issuer keys shall require the presence of multiple individuals, each fulfilling distinct roles. The entire process shall be formally documented.

6.1.1.2 Key pairs for e-identification holders

Keys for an e-identification are (usually) generated in connection with the issuance of the e-identification. The e-identification holder's private keys shall be stored in the e-identification with read and write protection. During certification, the integrity of the keys shall be verified. Key generation and associated checks (prior to certification) shall be carried out in such a way that the probability of key pair duplication is negligible or non-existent.

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

The Issuer, an Agent, or the RA function shall be responsible for the distribution of e-identifications. Each e-identification shall be protected by an initial PIN, which shall be delivered to the holder in such a manner that it is never presented together with the e-identification until received by the holder.

6.1.3 Delivery of the public key to the certificate issuer

The public key is generated by the Issuer.

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

The Relying party is responsible for obtaining the correct and valid versions of the CA's public keys (see chapter 2).

6.1.5 Key size

The key size for RSA key pairs generated in the CA system shall be at least 2048 bits.

6.1.6 Parameters for public key generation and quality control

The keys of the e-identification holder, which in the certificates are designated for encryption, authentication, and/or verification of non-repudiation, shall be assigned public exponents that prevent known attacks. The Issuer's keys shall likewise be assigned public exponents that prevent known attacks. The Issuer is expected to remain informed of developments in PKI technology and to adapt its cryptographic algorithms accordingly in order to maintain a high level of security.

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

CA certificates (including root certificates) shall have the keyCertSign and cRLSign bits set in the certificate's key usage field (see RFC 5280). Only the root certificate shall be permitted to issue CA certificates; such CA certificates shall have the pathLenConstraint set to 0 (see RFC 5280). Certificates of key holders used for message signing shall have the nonRepudiation bit set in the key usage field. This bit is also referred to as contentCommitment (see RFC 5280).

6.2 Private key protection and cryptographic module engineering controls

Private issuer keys intended for signing certificates, revocation lists, root certificates, and other private keys within the CA system shall be protected by strong physical safeguards (see chapter 5.1) and logical safeguards (HSM). Other private keys within the issuance process, which are used outside the CA system environment and affect certification issuance and revocation control services, shall be stored and used in smart cards (PKCS#15) and/or other secure modules (PKCS#12).

6.2.1 Standard and procedure for the use of a cryptographic module

The HSM used for key generation shall be certified at a minimum according to CC EAL4+ and FIPS 140-2 Level 3.

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

Physical access to the CA service's private issuer key shall require the cooperation of at least two individuals throughout the entire lifecycle of the key, from generation until all copies have been securely deleted. Certain sensitive operations shall likewise require the presence of more than one individual (see chapter 5.2.1).

6.2.3 Key escrow of the private Issuer key

Not applicable. The Issuer does not escrow any private keys, including private Issuer keys, RA administrators' private keys, or customers' private keys in issued e-identifications.

6.2.4 Backup of the private Issuer key

Private issuer keys intended for signing certificates, revocation lists, root certificates, and other private keys within the CA system shall be backed up.

The handling of the backup copy shall provide at least the same level of protection as the keys used in the production environment. At no time shall the backup copy be available in unencrypted form outside the HSM. The copy shall be securely stored, locked separately from the CA system, and access shall require the cooperation of two authorized individuals.

6.2.5 Archiving the private Issuer key

See chapter 6.2.3. and 6.2.4.

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

The private issuer key shall be generated within the cryptographic module specified in chapter 6.2.7 and shall never leave the module except for backup archiving or when being transferred to a new cryptographic module.

6.2.7 Storage of the private Issuer key in the cryptographic module

The issuer's private key shall be stored in an HSM module certified at least according to CC EAL4+ and FIPS 140-2 level 3. Access to the HSM module requires the simultaneous presence of at least two authorized people, in accordance with chapter 5.2.2.

6.2.8 Method for activating the private Issuer key

Activation of the CA service's private keys for root certificates requires the handling of two people and is performed only when new root certificates are to be created. Access to the HSM module is restricted (see chapter 5.1.2), and specific activation data shall be required in order to activate the Issuer's private 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 shall be destroyed when its validity period has expired or if it has been revoked. This is done by permanently deleting the private key in the HSM and destroying the backup copy of the private key. However, Issuer keys shall not be destroyed if this would conflict with the archiving requirements in the certificate policy or with requirements in other legislation.

6.2.11 Security evaluation of the cryptographic module

No formal security evaluation is required, as long as the module meets the requirements in chapter 6.2.1.

6.3 Other aspects of key pair management

No sensitive information from the CA, key generation, or personalization processes may leave the systems in a manner that conflicts with this policy. The creation of private keys on a smart card takes place in a protected environment and requires the participation of at least two authorized individuals. During maintenance and similar situations where the described protective measures cannot be guaranteed, storage media containing sensitive information shall primarily not be sent along, and if this cannot be avoided, shall be securely erased. Decommissioned storage media shall be physically destroyed.

6.3.1 Archiving the public key

All public keys shall be archived by the Issuer; this applies both to Issuer keys and to the public keys of issued e-identifications, (see chapter 5.5.2).

6.3.2 Validity period for e-identifications and key pairs

The CA service's key pair and root certificate have a validity period of 12 years.
Issued e-identifications and their key pairs have a validity period of 2 years.

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

The e-identification may not be used by anyone other than its holder. The e-identification is protected by a security code (PIN), which is required for its use. The e-identification holder must keep this code in a secure manner and not disclose it to anyone. If there is any suspicion that an unauthorized person may have gained access to the e-identification, it must be immediately revoked.

6.4 Activation data

6.4.1 Generation and installation of activation data

The input to all generation processes for activation data shall be a random number.

6.4.2 Protection of activation data

Activation data for the CA service's private issuer key shall be protected against theft and fire. Only trusted individuals shall have access to the activation data.

6.4.3 Other aspects of activation data

Not applicable.

6.5 Computer security controls

The operating environment for the CA service shall be designed to achieve a high level of security, which means that it should physically and logically be separated from the Issuer's other operations. The tasks performed in the operating environment are software updates, starting and stopping applications, other system maintenance, and work involving the handling of CA keys. The administration of the CA service shall be structured in such a way that individual roles according to chapter 5.2 can be separated. Separation of roles at the OS level can be ensured through dual control. Logging into the CA service shall be done with separate user identities to ensure traceability both at login and during the RA administrator's continued work in the system. The security functions should ensure access control and traceability for each administrator at an individual level for functions that affect the use of the Issuer's private key. RA functions concerning the issuance and revocation of e-identifications or certificates shall be carried out via a web interface towards the CA service, which requires that the requested action be signed with the RA administrator's e-identification.

6.5.1 Special IT security requirements

Initialization of the system that uses private issuer keys shall require the cooperation of at least two trusted people. A detailed log shall be kept of all manual steps in the process.

Installation of the operating system and the CA system shall take place immediately after disk formatting and with the vendor's original release of the software. A record of the installation and configuration process shall be signed by all participants and archived. When registering initial user authorizations in the CA system, at least two individuals in trusted roles shall cooperate.

6.6 Life cycle security controls

6.6.1 Security requirements for system development

The development of software that implements functionality of the CA system shall be carried out in a controlled environment where the supplier applies a quality assurance system to protect against the introduction of unauthorized code.

6.6.2 Security requirements for security administration

Configuration and modification of the CA system shall be documented in the form of logs. Security administration shall only be performed by person(s) assigned the role to handle this, see chapter 5.2.

6.7 Network security controls

The CA service should be connected to an external network and protected by a dedicated firewall with sufficient strength to withstand DoS/DDoS attacks and similar threats that may be directed against the service. The CA service's firewall should be configured to allow only the protocols necessary to realize the CA function. Furthermore, the CA service and its web portal should be connected via (at least) two separate connections to increase availability and operational reliability. Communication to and from the CA environment shall use encryption of a strength that is considered reliable according to prevailing best practices.

6.8 Timestamping

The CA system shall have access to an accurate time source that meets operational requirements for creating certificates, revocation lists, and logs.

7 Certificate, CRL, and OCSP profiles

Certificates and revocation lists shall comply with the X.509 version 3 standard.

7.1 Certificates that the Issuer may issue

All issued e-identifications' public and private keys shall have a key length of at least 2048 bits (see chapter 6.1.5).

The issuance of e-identifications in accordance with this policy entails that:

1. E-service identification Card shall be issued only to physical individuals (not to organizations or authorities).
2. E-service identification Card comply with the PKCS#15 standard, shall be protected by a PIN and be stored on a smart card.

7.1.1 E-service Identification Card (personal)

The E-service identification File is a personal, card-based electronic e-identification, based on the PKCS#15 standard, issued to a physical individual within a customer organization.

The e-identification may be regarded as the electronic equivalent of a physical company or organizational identification card, guaranteeing the individual's affiliation with a specific company or organization. It is used for identification, system and application logins, encryption, and the signing of electronic transactions.

The E-service identification Card is personal, has a validity period of two years, and contains two certificates with associated cryptographic keys. The e-identification is protected by a PIN, which applies both to authentication and to signing. The e-identification has two PIN: one for authentication and one for signing. The physical smart card may be provided with a visual print displaying the holder's name, the organization's name, the organization's logo, and the validity period of the e-identification. Other types of prints may also occur.

7.2 Certificate profile

The certificate standard is X.509 v3.
The presence and use of data elements in the certificates shall comply with this policy.

7.2.1 E-service identification Card (personal)

Certificate fields:

Field name	Occurrence	Comment/Value
Version	M	=2 (X.509 v.3)
SerialNumber	M	The Issuer uses a serial number starting from 1000 and upwards.
Signature	M	SHA256WithRSAEncryption
Issuer	M	The following attributes are used - countryName (SE) - OrganisationName (Expisoft AB) - CommonName (ExpiTrust e-Tjanstelegitimationer kort CA v4)
Validity	M	A validity period of (at least) two years.
Subject	M	The following attributes are used - countryName (SE) - organisationName (Official customer name for the organization, company, authority, etc.) - title (Title specified when ordering the e-identification.) - surname (Surname specified when ordering the e-identification.) - givenName (First name specified when ordering the e-identification.) - SerialNumber (Organization number: 10 digits followed by a number, often an employee number, Format: 16 XXXXXXXXXX<nr>)

		- CommonName
Subject PublicKey Info	M	RsaEncryption (2048 bits key)

The following certificate extensions are used in issued e-identifications

Field name	Occurrence	Critical	Comment/Value
authorityKeyIdentifier	M	non-critical	SHA-1 (hash of the CA service's public key)
subjectKeyIdentifier	M	non-critical	SHA-1 (hash of the certificate's public key)
keyUsage	M	critical	- digitalSignature - nonRepudiation - keyEncipherment - dataEncipherment
certificatePolicies	M	non-critical	PolicyIdentifier=1.2.752.54.9.2.13.2
Ext Key Usage	M	non-critical	Följande attribut används: - emailProtection - ClientAuth ipsecEndSystem
CRL Distribution Points	M	non-critical	http://cdp1.certservice.se/cdp/eid/ExpiTrust%20e-Tjanstelegitimationer%20Kort%20CA%20v4.crl http://cdp2.certservice.se/cdp/eid/ExpiTrust%20e-Tjanstelegitimationer%20Kort%20CA%20v4.crl
Subject Alt Name	O	non-critical	If email addresses are entered here, they shall comply with RFC 5322 (local-part@domain). The IP address of VPN equipment may be specified in this extension.
Subject Directory Attributes	-	non-critical	Not currently in use
authorityInfoAccess	M	non-critical	http://ocsp.certservice.se

The following private extensions are used in issued e-identifications

Field name	Occurrence	Critical	Comment/Value
Card Number	O	non-critical	Not currently in use

No private extensions are currently used in issued e-identifications.

7.3 CRL Profile

The CA service issues revocation lists that comply with CRL version 2 according to X.509.

7.4 OCSP Profile

OCSP is provided for the validation of certificates. OCSP requests are signed with a certificate dedicated to the OCSP server and not by the respective root certificate.

The DNS address for OCSP is “ocsp.certservice.se”. Since the OCSP request is digitally signed, the HTTP protocol is used to access the service.

8 Compliance audit and other assessments

8.1 Frequency and circumstances of review

The Certification Authority Administrator (CAA) (see chapter 5.2.1) determines the frequency and circumstances for internal and external audits to ensure compliance with this policy. The Issuer reserves the right to periodically require inspections and audits of the CA service’s subcontractors, Resellers, Administrators, and RA function to validate that they operate in accordance with the security practices and procedures specified in this CP and CPS.

8.2 Identity/qualifications of auditors

The Certification Authority Administrator (CAA) appoints the auditor.

8.3 Auditor's relationship to the assessed entity

See chapter 5.2.4.

8.4 Areas for audit

During an audit, the following areas shall be reviewed:

- The CA service’s functionality regarding identification and authentication.
- The CA service’s operational functions.
- The CA service’s procedural and personnel controls.
- The CA service’s physical and technical security.

The review shall also cover:

- The suitability of the Certification Practice Statement (CPS) and its compliance with this Certificate Policy (CP).
- The practical implementation of the Certification Practice Statement (CPS).
- Compliance with agreements and collaborative arrangements concerning the CA service’s Resellers and subcontractors.

8.5 Actions taken as a result of a detected deficiency

Based on the compilation of any identified deficiencies, a plan of corrective actions shall be developed under the direction of the Certification Authority Administrator (CAA), see chapter 5.2.1.

8.6 Communication of audit results

The compilation and corrective actions according to chapter 8.5 are not published publicly, but the audit results shall be provided upon request by a Relying party. The report shall include information about all identified deficiencies of such a nature that they may be considered to affect a Relying party's trust in an issued e-identification. The information shall include the type of deficiency as well as an assessment of potential risks and consequences.

However, the report must not contain detailed information about the CA service or any deficiencies that could be considered to compromise the security of the system.

9 Other business and legal matters

9.1 Fees

9.1.1 Fees for the issuance of e-identifications

The fee shall be displayed when ordering the e-identification or be known through separate agreements with the customer.

9.1.2 Fees for access to certificates

Not applicable.

9.1.3 Fees for access to revocation information

Included in the basic service.

9.1.4 Fees for other services

According to separate agreements, where 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 regulated in 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 regulated in 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 policy, 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

The CA shall provide CA services in accordance with this CP.

9.6.2 RA's obligations and warranties

The RA shall perform identification and registration tasks in accordance with this CP.

9.6.3 Obligations and warranties of e-identification holders

In cases where the e-identification holder generates their own key pairs, those keys shall be generated with high quality and protected against disclosure and unauthorized use.

The e-identification holder, the Requester, or their organization shall pay the Issuer the agreed fee for the e-identification.

9.6.3.1 Temporary suspension of e-identification

If an e-identification holder has not paid an invoice after three reminders, the Issuer reserves the right to temporarily suspend the e-identification and its associated certificate. Once the invoice has been paid, the temporary suspension will be lifted, and the e-identification can be used again.

9.6.4 Obligations and warranties of the Relying party

When verifying signatures, the validity of the certificate shall be checked. This also includes verification against the revocation list.

9.6.5 Obligations and warranties regarding other participants

Not applicable.

9.7 Disclaimers of warranties

The issuance of an e-identification in accordance with this policy shall not cause the Issuer to be regarded as an agent, proxy, or otherwise as a representative of the e-identification holder or the Relying party.

9.8 Limitations of liability

The Issuer assumes no liability for unauthorized use of certificates (see chapter 1.3).

9.9 Indemnities

Not applicable.

9.10 Term and termination for this Certificate Policy (CP)

9.10.1 Commencement of the period

This Certificate Policy shall be effective upon its publication on the Issuer’s website.

9.10.2 Termination of the period

This Certificate Policy 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 policy or the associated Certification Practice Statement (CPS).

9.12 Amendments of this Certificate policy

See chapter 1.4.

9.13 Dispute resolution procedures

Any dispute arising from this Certificate Policy 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 policy 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 CP.

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.

Approved by:	CEO, Christina Pettersson	Date:	2025-09-30

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
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.