Swedish Public Sector Certificate Policy

Key Information:

Formal title:	Swedish Public Sector Certificate Policy
OID:	1.2.752.146.200.2.1.0.0 { iso (1) member (2) sweden (752) swedish social insurance agency (146) EFOS (200.2) [cpvn-top (0) cpvn-2nd (0) cp (1)] }
Responsible authority:	EFOS Policy Authority
Version:	*1.1.6*
Effective date:	*2021-02-22*
Classification / Distribution	Un-classified / Unlimited distribution
Published at:	https://repository.efos.se
Author:	EFOS Policy Authority
Point-of-Contact:	Försäkringskassan, SE-851 93 Sundsvall, Sweden email: EfosPA@efos.se

Approval record:

Version	Date	Approved (role)	Reason / notes
1.1.6	2021-02-22	EFOS PA	Approved
1.1.5	2021-02-08	EFOS PA	Changes in several chapter to add RPA certifikates
1.1.4	2020-08-31	EFOS PA	Approved
1.1.3	2020-08-19	EFOS PA	Changes in chapter 1.4.1, 8.2 and 8.4
1.1.2	2020-03-24	EFOS PA	Approved
1.1.1	2020-02-28		Changes to reflect EFOS Tillitsramverket, in chapter 9.10.2 and other small changes
1.1.0	2019-10-09	EFOS PA	Approved
1.0.1	2019-09-19		Minor changes. Changed Efos to EFOS and from portalen to portal. Change in chapter 4.9.7 and update in chapter 5.2.1. Update Figure 1.
1.0.0	2019-06-10	EFOS PA	Approved
0.9.0	2019-06-10		Changed after comments
0.8.0	2019-05-16		RFC

CONTENTS

1. INTRODUCTION

1.1. Overview

All special terms and definitions addressed in 1.5.2 apply from hereon.

"**E-id for the Swedish public sector**" hence referred to as EFOS is a PKI that accommodates a large, public, and widely distributed community of users within the public sector of Sweden that have diverse needs for IT- and information security. Försäkringskassan offer PKI subscriber services to organizations that have signed an EFOS membership agreement with Försäkringskassan (Swedish Social Insurance Agency). This contract must make references to this CP and the EFOS trust framework which defines the conditions under which certificates can be issued. This contract will also regulate the rights and obligations for each part in the contract. As part of this CP and the contract all accountable issuers must apply for their membership with a declaration of assurance. Each accountable issuer and its declaration of assurance are subject to review by the EFOS Policy Authority.

An **accountable issuer** may have sub-contractors that need end-entity certificates from EFOS. Such sub-contractors shall have an agreement with the accountable issuer and are referred to as Third party organizations.

An **EFOS issuance domain** is an entity that consists of one accountable issuer and any third parties that they have a signed contract with.

Individuals, organizations and functions that use EFOS certificates are referred to as a relying party. Each relying party must rely on a certificate in accordance with the terms set forth in the relying party agreement.

1.1.1. Certificate Policy

This document sets forth the Certificate Policy (CP) addressing the provision of certificates for Swedish Public Sector by the Swedish Public Sector Certificate Authority operated by Försäkringskassan (Swedish government's Social Insurance Agency), and for the life-cycle management of those certificates. The certificates shall be issued from the 'Swedish Public Sector Person 2 CA', 'Swedish Public Sector Person 3 CA', 'Swedish Public Sector Person 4 CA', 'Swedish Public Sector Function CA', 'Swedish Public Sector RPA CA' and 'Swedish Public Sector Mobile ID CA'. This policy is published under the authority of the EFOS Policy Authority, hence referred to as EFOS PA, whose executive mandate is defined in the EFOS Policy Authority [EFOS PA charter].

For public references, the English-language title (and associated abbreviation) of Försäkringskassan and E-identitet för offentlig sektor (EFOS) shall be used.

This CP conforms to the Internet Engineering Task Force (IETF):

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

This Certificate Policy is subject to compliance audits in accordance with chapter 8.

1.1.2. Certification Practice Statement

This policy may be referenced by any Certification Practice Statement (CPS) fulfilling the obligations herein. Specifically, the Swedish Public Sector Certification Practice Statement [EFOS CPS] fulfils all the obligations of this policy.

Within EFOS, certificates are issued according to different certificate profiles that govern certificate contents and possible subscribers.

A subordinate CA that operates within EFOS must publish a Certification Practice Statement (CPS) that is approved by the EFOS Policy Authority. A CA without an approved CPS will not become a part of EFOS.

1.1.3. Scope of Applicability

This CP covers Swedish Public Sector CA Public Key Infrastructure which issues certificates to EFOS subscribers.

This document is targeted at:

- Certificate Authorities that operate within EFOS.
- Accountable issuers that operate within EFOS.
- Third parties within an issuance domain
- EFOS PKI service providers and processing centre that operate in terms of a Certification Practices Statement (CPS) that complies with the requirements in this CP.
- Relying parties who need to understand how much trust to place in an EFOS certificate, or a digital signature using a EFOS certificate.
- Auditors that conduct audits of different parts of EFOS.

Figure 1 offers a schematic representation of the EFOS PKI document structure.

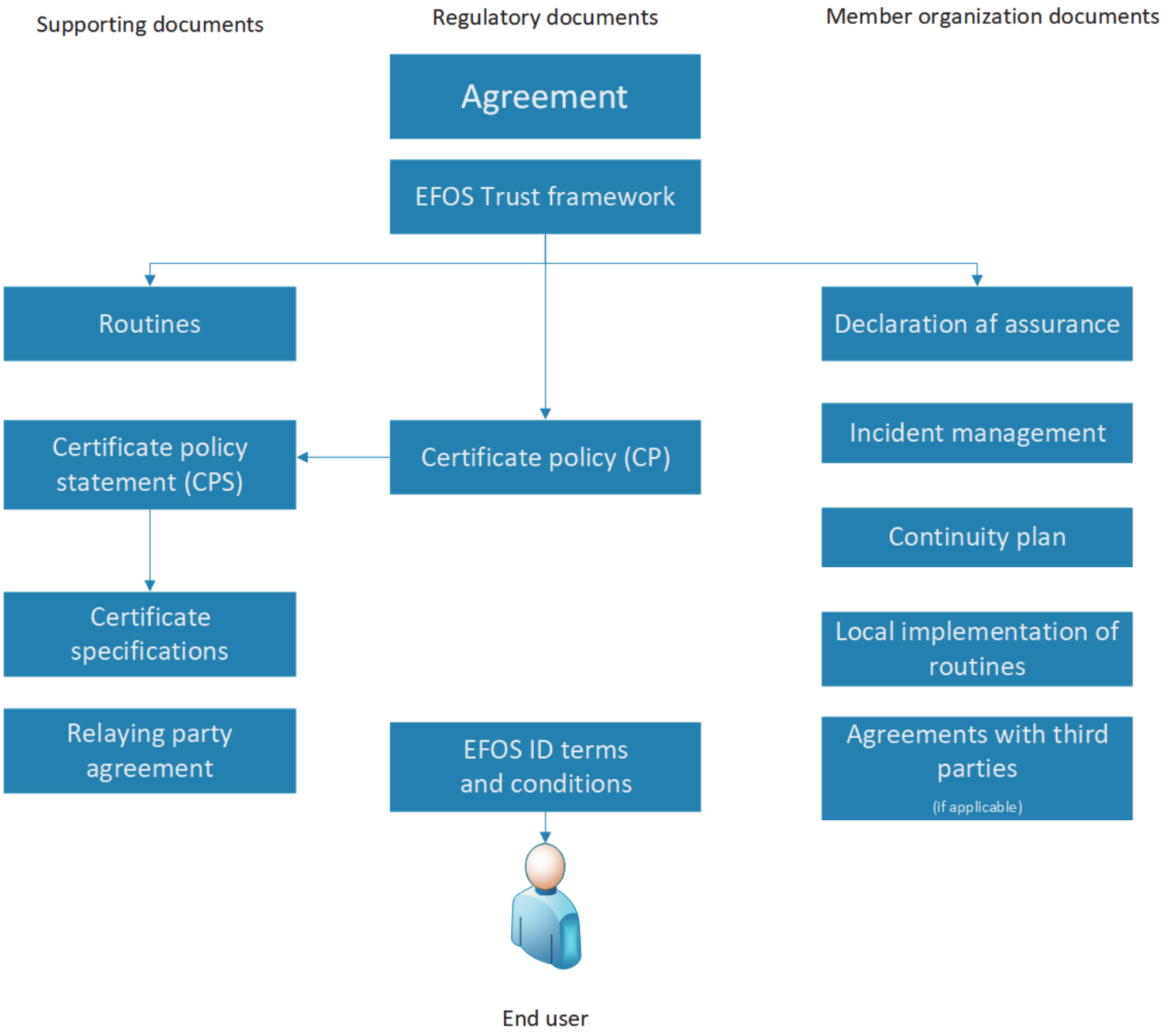

Figure 1 – EFOS PKI document structure

Certificates issued pursuant to this CP are intended for use within the Swedish Public Sector. This includes the subcontracted service providers and subcontracted personnel within each issuance domain, hereafter assumed to be included within any reference to the Swedish Public Sector.

Any use of or reference to this CP outside the scope of the EFOS PKI is exercised completely at the using party's

own risk. Only the EFOS PKI may assert the OIDs listed in Section 1.2 of this CP.

This CP presents multiple levels of identity assurance and covers the issuance of Certificates for the following purposes:

- Individuals e.g. users – Authentication and signing certificates to smart cards and mobile devices intended to identify physical persons
- Functions – TLS certificates for machines, servers and shared email addresses intended to identify non-human entities

1.2. Document name and identification

The OID for the EFOS PKI is derived thus:

Försäkringskassan	::= { iso (1) member-body (2) sweden (752) swedish social insurance agency (146) } 1.2.752.146
EFOSRootCA	::= { SSIA 1.0 } 1.2.752.146.200

Policy OIDs addressed by this CP are:

Swedish Public Sector Person 2 CA v1	::= { EFOS –Person 2 CA 100 } 1.2.752.146.210.2
Swedish Public Sector Person 3 CA v1	::= { EFOS –Person 3 CA 100 } 1.2.752.146.220.3
Swedish Public Sector Person 4 CA v1	::= { EFOS –Person 4 CA 100 } 1.2.752.146.230.4
Swedish Public Sector Function CA v1	::= { EFOS – Function CA 100 } 1.2.752.146.240.2
Swedish Public Sector Mobile ID CA v1	::= { EFOS – Mobile ID CA 100 } 1.2.752.146.250.3
Swedish Public Sector RPA CA v1	::= { EFOS – Mobile ID CA 100 } 1.2.752.146.260.2

In order to provide a discrete OID for this document and the corresponding CPS the following schema has been devised to identify the current formal release of these documents, as follows:

Current Formal Release	Version
EFOS Tillitsramverk	{EFOS- Tillitsramverk } 1.2.752.146.200.1.x.y.1
EFOS CP	{EFOS-CA cpvn-top cpvn-2nd } 1.2.752.146.200.2.x.y.1
EFOS CPS	{EFOS- CA } 1.2.752.146.200.3.x.y.1

These OID relationships are shown schematically in Figure 2, in context with other CAs falling under the authority of the EFOS Policy Authority.

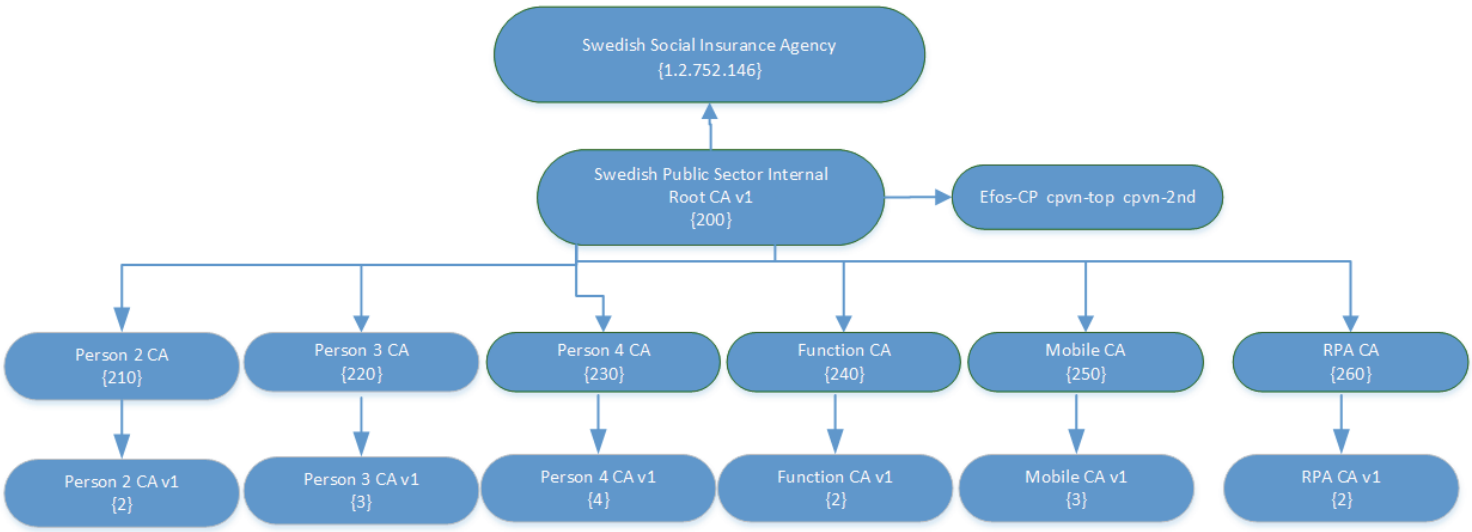

Figure 2 – EFOS PKI OID hierarchy

This CP shall apply to any entity asserting any of the above-defined policy OIDs.

1.3. PKI Participants

This section describes the entities relevant to the administration and operation of the EFOS PKI.

1.3.1. Certification Authorities

The term Certification Authority (CA) is an all-embracing term that refers to all entities authorized to issue public key certificates within EFOS

1.3.1.1. EFOS Policy Authority

The EFOS Policy Authority are responsible for the following:

a) Management of initial drafting and subsequent amendments to the EFOS CP when necessary or at least every 12 months
b) Review and approval of top-level versions of the EFOS CP, prior to them becoming operationally effective
c) Commissioning of audits of the policy management and operations of the EFOS PKI so as to maintain the certifications required by this CP
d) Taking action to ensure policy-related audit recommendations are implemented
e) Approval of, and ordering maintenance of the EFOS CPS
f) Ordering, if necessary, the adaptation of CAs as EFOS CP and CPS change

The chairman of the EFOS Policy Authority shall be appointed by EFOS Policy Authority. A complete description of EFOS Policy Authority roles and responsibilities is provided in EFOS PA charter.

1.3.1.2. EFOS Policy Working Group

The EFOS Policy Working Group is established to undertake developmental work and analysis, as follows:

a) Identification and drafting of internally-originating proposals for changes to this CP;
b) Review of received proposals for changes to this CP;
c) Recommendations to the EFOS Policy Authority for approval or rejection of any such changes; and
d) Compliance analysis and recommendations for approval by the EFOS PA of EFOS CPS and any other

CPS. The EFOS Policy Working Group shall be chaired by the chairman of EFOS Policy Authority.

1.3.1.3. EFOS Operational Authority

The EFOS Operational Authority (EFOS OA) is responsible for the daily operations of the CA. It is divided into Technical Operations and Functional and Administrative Operations. EFOS Technical OA shall be headed by the EFOS OA

Technical Manager who shall report to EFOS PA.

There is one EFOS Functional and Administrative OA at Försäkringskassan. Both functions shall report to EFOS PA.

Technical operations include:

a) Drafting, maintenance and submission for approval of the EFOS CPS;
b) Maintaining the certificates and CRLs recorded in the EFOS PKI Repository;
c) Performing back-ups and ensuring the readiness of all back-up facilities;
d) Ensuring the on-going availability of all CA services and facilities in accordance with EFOS CP and CPS;
e) Taking action to ensure that audit recommendations concerning operational practices are implemented;
f) Administration of the technical components of the RA-client

Functional and administrative operations include:

a) Monitoring the EFOS OA adherence to this CP and execution of audits required by the obligations set forth in this CP
b) Ensure and administer the process of establishing, updating and terminating issuance domains within the EFOS PKI
c) Ensure adherence to the agreed Service Level Agreement set forth in the agreement with Försäkringskassan regarding the EFOS PKI
d) Ensure adherence to the agreements with subcontractors involved in the development and operations of the EFOS PKI
e) Administration of rulesets for function certificates

Trusted roles within the EFOS OA are defined in 5.2.1.

1.3.2. Registration Authorities

Registration Authorities (RA) can refer to either the organization or the person ultimately responsible for certificate issuance within an issuance domain. RA's are hence referred to as accountable issuers. Individuals assigned to this role shall be appointed by a representative with the appropriate mandate in their organization. An issuance domain may consist of one or many organizations operating within the Swedish Public Sector. All issuance domains must adhere to the EFOS trust framework and the terms in the EFOS membership agreement.

1.3.3. Subscribers

Subscribers under EFOS include all end entities of certificates issued by an EFOS CA. A subscriber is the entity named as the end entity subscriber of a certificate. End entity subscribers may be:

- Individuals – e.g. physical persons within an issuance domain
- RPA – e.g. digital Robot/RPA within an issuance domain
- Functions – e.g. infrastructural components such as firewalls, routers, trusted servers or other devices.

Subscribers that are individuals must agree to the EFOS Terms and Conditions.

In case of functions the EFOS function terms and conditions must be agreed upon by the person that issues the certificate

1.3.4. Relying Parties

Relying parties are individuals, organizations and functions that use EFOS certificates. For example a service that uses the information in a certificate and has to make a decision whether to trust/rely in it or not. Each relying party must rely on a certificate in accordance with the terms set forth in the relying party agreement.

Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate.

Relying parties that are not part of an issuance domain, and wish to use EFOS Out-of-band authentication service, hence referred to as EOOBAS, must sign an additional agreement designed for this purpose.

1.3.5. Other Participants

1.3.5.1. Auditors

The EFOS PKI will require the services of other security authorities, such as compliance auditors. Such auditors are appointed by the EFOS Policy Authority.

1.3.5.2. Processing centres

Processing centres are entities that are not CA but participate in the issuance process of certificates.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

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

This CP covers different types of end entity certificates/tokens with varying levels of identity assurance. Identity assurance levels for a certificate may vary over time and the current mapping between certificate OID's and the matching identity assurance level can be found in figure 3.

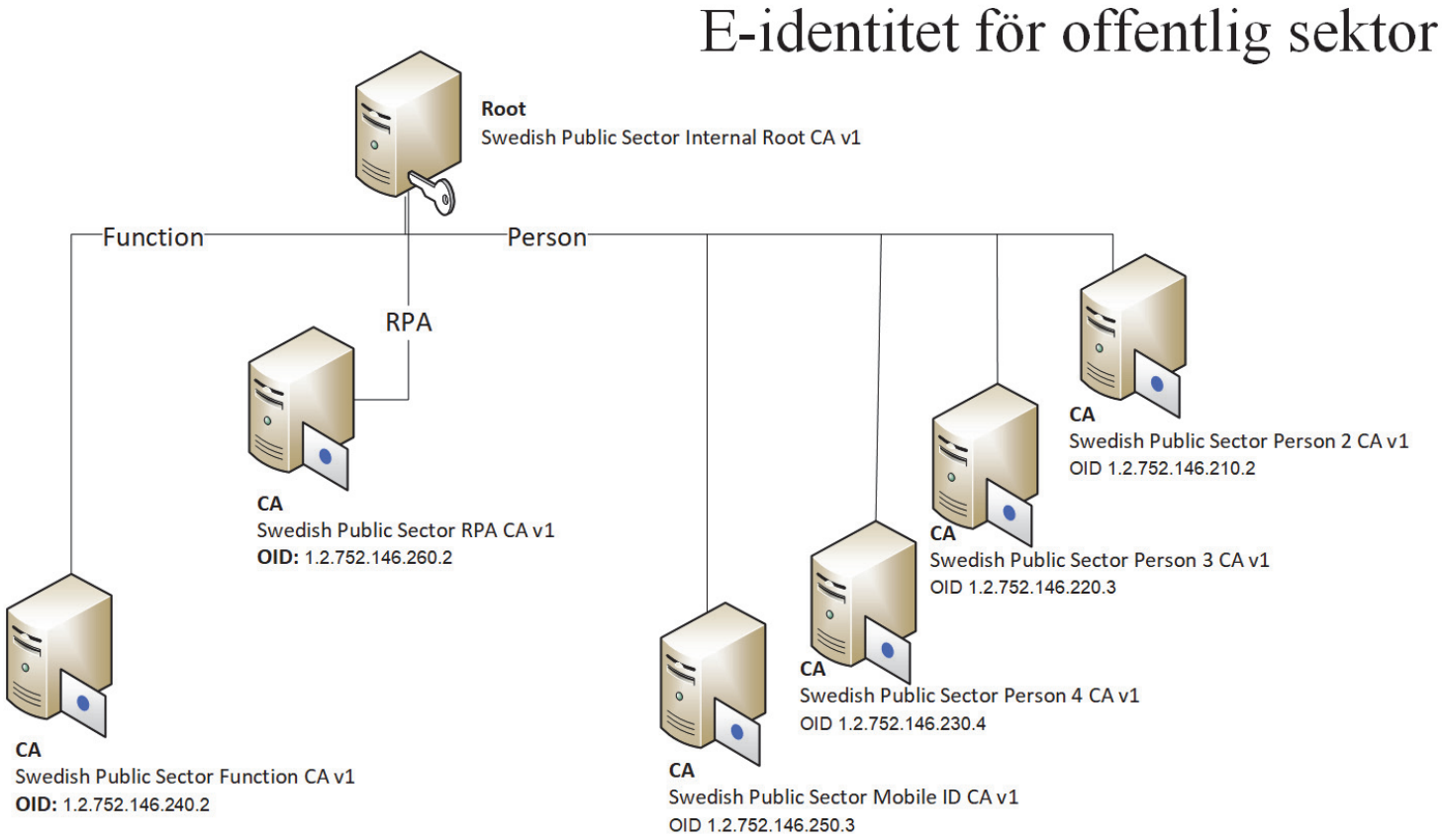

Figure 3 – EFOS PKI mapping between certificate OID's and assurance level

The following table provides a brief description of the appropriate uses of each type of certificate.

Certificate/Token type	Appropriate Use
Authentication Certificates for individuals	These certificates are used to identify the Subscriber stated in the subject of the certificate, when used for Authentication/ identification within the public sector. Any other use is not permitted. These types of certificates are issued from the following CAs: - Swedish Public Sector Person 2 CA v1 - Swedish Public Sector Person 3 CA v1 - Swedish Public Sector Person 4 CA v1 - Swedish Public Sector Mobile ID CA v1
Signing Certificates for individuals	These certificates are used to identify the signature of the Subscriber stated in the Signing Certificate, when used for signing, signature or encryption within the public sector. Any other use is not permitted. These types of certificates are issued from the following CAs: - Swedish Public Sector Person 2 CA v1 - Swedish Public Sector Person 3 CA v1 - Swedish Public Sector Person 4 CA v1 - Swedish Public Sector Mobile ID CA v1
Authentication Certificates and Signing Certificates for Functions	These certificates are used to identify machines, servers and shared email addresses. These certificates are issued from the following CA: - Swedish Public Sector Function CA
Authentication Certificates and Signing Certificates for RPA/Robots	These certificates are used to identify robots, RPA, ChatBots, Digital Assistans and equal. These certificates are issued from the following CA: - Swedish Public Sector RPA CA

1.4.2. Prohibited Certificate Uses

Certificates do not attest to the good behaviour of the certificate Subjects and Subscribers. They shall not be taken to guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with.

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

a) where prohibited by any laws, be they national, European or international.
b) where the usage does not correspond the Key Usage and/or the Extended Key Usage stated in the certificate
c) certificates issued to functions shall not be used to identify persons and vice versa.

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

1.5. Policy Administration

1.5.1. Organization Administering the Document

The 'Responsible authority' cited on the cover page shall be responsible for the administration of this CP.

1.5.2. Contact Person

The 'Point-of-contact' cited on the cover page, shall be the initial point of contact for all matters.

1.5.3. Person determining CPS suitability for the policy

The 'Responsible authority' cited on the cover page shall determine the suitability of the [EFOS CPS].

1.5.4. CP Approval Procedures

Each formal release of this CP requires approval by EFOS PA whose signature shall be applied to an electronic version

of it.

Version identification has three levels requiring the approval authority identified below according to level. Version identification is simple integer sequencing at each level.

Top-level: A formal release of this CP which has a **significant policy change** requiring a change of the policy's OID

Second-level: A formal release of this CP which has a **no significant policy change** and therefore does NOT require a change of the policy's OID

Third-level: A draft of this CP intended for review and/or recommendation as the next formal release

When the identification at a given level is incremented all subordinate levels revert to zero. Only the first two levels need be shown in formal releases (level three is by default zero in any formal release). During the drafting of revisions this record shall record all draft versions and their approvals until such time as a formal release is approved.

On its effective date a formal version of this CP shall become the applicable version of the policy for all operational purposes and shall supersede all previous versions which shall thereby become redundant. The EFOS Policy Authority shall preserve records of all past versions.

1.6. Definitions and Acronyms

Unless alternative definitions, meanings or interpretations are assigned in the following parts of this sub-clause, the definitions in CABF and RFC 3647 apply. Should there be any conflict between terms defined in both these documents, CABF shall take precedence.

Term	Explanation
Accountable issuer	The person responsible for certificate issuance within an issuance domain
Authorized applicant	Person authorized to request a function certificate
CABF	CA Browser Forum
Coordination number	Swedish unique identifier for a person (samordningsnummer)
Declaration of assurance	Compliance statement regarding EFOS trust framework (Tillitsdeklaration)
EFOS	E-identitet för offentlig sektor (Swedish Public Sector Certificate Authority)
EFOS CA	Function for issuing certificates within EFOS
EFOS PA Charter	Rules for EFOS PA
EFOS PKI	Public key infrastructure framework for EFOS
EFOS-portal (Portal)	Administration interface for EFOS
EOOBAS	EFOS Out-of-band authentication service
Function certificate	Certificate issued for a non-person, e.g. a server
IAA	Inter-Agency Agreement (IAA). Eligible Agencies or organizations wishing to participate in the EFOS PKI shall signify their acceptance of the terms of an agreement.
ID-administrator	Collection name for all roles within EFOS, that check ID and issues certificate/smart card
Individual certificate	Certificate issued for a person
Issuance domain	An entity that consists of one accountable issuer and any third parties that they have a signed contract with
Level of Assurance (LoA)	A Level of Assurance, as defined by the by ISO/IEC 29115 Standard, describes the degree of confidence in the processes leading up to and including an authentication. See https://www.elegnamnden.se/elegitimering/kvalitetsmarketsvenskelegitimation/omtillitsnivaerforelegitimering.4.4498694515fe27cdbcf101.html
Membership agreement	Legal agreement that regulate the rights and obligations for each part of EFOS
Personal identity number	Swedish unique identifier for a person (personnummer)
RPA	Robot, ChatBot and more are hence referred to as "RPA".
Relying Party	Limitations defined in §1.3.4 but otherwise with the meaning ascribed to it in [RFC3647].
Sequential number	Unique identifier(ordningsnummer) for a person that don't have Personal identity Number/Coordination number.
StatsRegister	Statistiska centralbyrån (Statistics Sweden) [StatsRegister], available at

	http://www.myndighetsregistret.scb.se/Myndighet or equal.
Subscriber	User of certificate
Third party	Sub-contractors that need end-entity certificates and have an agreement with the accountable issuer
Trust framework	The common requirement that governs EFOS (Tillitsramverk)

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

EFOS Operational Authority is responsible for making information regarding the EFOS PKI available according to the following:

- **Regulatory documents** (Trust framework, CP, CPS, Certificate profiles, issuance routines, AIA, CRL i.e.) – see https://repository.efos.se/
- **Declaration of assurance and audit information** – Not published.
  Are kept in a separate tool.

2.2. Publication of certification information

Each Responsible Entity shall ensure that information for which it has a publishing responsibility shall be available through a publically accessible, on-line, repository.

2.3. Time or frequency of publication

All information, including changes in the regulatory documents, is published promptly after it is decided within the EFOS PKI. Regulatory documents are reviewed by the EFOS Policy Authority when necessary or at least every 12 months.

2.4. Access controls on repositories

Regulatory documents, AIA, CRL and OCSP shall be provided with unrestricted read access.

EOOBAS is provided using Mutual TLS for relying parties that are entitled to access.

Repositories must implement logical and physical controls to prevent unauthorized modification to such repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

EFOS CAs shall issue certificates with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards.

Every subscriber identity is registered along with a set of attributes. Identities and attributes are verified by involved RAs.

For EFOS function certificates additional rulesets for each RA are applied and verified by validation specialists based on the rules determined by OA.

The composition of names for different types of certificates are defined in the certificate profiles.

3.1.2. Need for Names to be meaningful

Distinguished Named in EFOS are ensured to be unique by means of a unique identifier. The unique identifier is contained within the Subject Serialnumber and serves as the general identification attribute for the end entity subscriber. For EFOS the unique identifiers are defined as follows:

- **For individuals** – A Swedish personal identity number, coordination number or a sequence number.
- **For RPA –** A unique ID generated by the EFOS-portal
- **For functions –** A unique ID generated by the EFOS-portal

The country attribute specifies the scope of other attributes contained within a certificate. This means that all attributes must be defined and be interpretable within each country.

Locality is defined as follows:

- **For functions** – the municipality where the Board of Directors of the organization that owns the function, for example a domain-name, has its seat.
- **For RPA** – one of the following
    - the municipality where the Board of Directors of the third party or the accountable issuer has it seat
- the county of the third party or the accountable issuer
- **For individuals** – one of the following
    - the municipality where the Board of Directors of the third party or the accountable issuer has it seat
    - the county of the third party or the accountable issuer

Organization is defined as follows:

- **For functions** – the name of the organization that owns the function
- **For RPA –** the organization name of the third party or the accountable issuer
- **For individuals –** the organization name of the third party or the accountable issuer

Subscriber is defined according to 1.3.3

Email addresses can only be expressed as SMTP-addresses (IETF RFC 2822 or IETF RFC 5322)

3.1.3. Anonymity or Pseudonymity of Subscribers

Subscribers shall not use anonymous or pseudonymous names.

3.1.4. Rules for interpreting various name forms

Distinguished Names in Certificates shall be formed and interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness of names

Distinguished Name uniqueness is ensured by the use of the Subject Serial number as described in 3.1.2

3.1.6. Recognition, Authentication, and role of trademarks

Certificate applicants shall not use names in their certificate applications that infringe upon the intellectual property rights of another entity. Explicitly, no certificate request may use any trademark, nor the identifying marks of any entity other than the one issuing the request.

Försäkringskassan shall not be required to determine whether a certificate applicant has intellectual property rights to the name appearing in a certificate application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name or trademark.

EFOS Policy Authority and EFOS accountable issuers shall be entitled, without liability to any certificate applicant, to reject or suspend any certificate application because of such disputes.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the certificate. The EFOS CA shall verify that the certificate applicant possesses the Private Key corresponding to the Public Key. How this is done varies depending on the used EFOS issuance routine.

3.2.2. Authentication of Organization Identity

Organizations cover all organizations within an issuance domain. Organizations within an issuance domain are verified with the Swedish Companies Registration Office and/or the Central Bureau of Statistics.

- **For individuals:**
    - EFOS policy authority verifies accountable issuers upon initial application and through audits
    - Accountable issuers verifies third parties
- **For RPA:**
    - EFOS policy authority verifies accountable issuers upon initial application and through audits

- **For functions:**
    - Validation specialists verifies in accordance with the EFOS function validation routine. Verified functions are included within a ruleset that is unique per subscriber name, organization and type of certificate and that enforces the correct organization information.

3.2.3. Authentication of Individual Identity

For any certificate application an entity's identity shall be verified in accordance with the EFOS issuance routines and the EFOS trust framework.

All individuals that receive a certificate must have a professional correlation with at least one of the organizations within an issuance domain. For all identity assurance levels, the professional correlation of each individual shall be asserted by means of manual or automated control in local employment register or automated control with organizations specific directory.

All individuals with a Swedish personal identity number or a Swedish coordination number are verified with the Swedish Tax Agency by the EFOS PKI.

For identity assurance level 3[1] or higher the individual must have a verified Swedish personal identity number.

3.2.4. Non-verified Subscriber information

No stipulation.

3.2.5. Validation of Authority

The EFOS PKI shall validate the authority of an entity requesting any type of certificate by verifying that they are either the requesting id-administrator or an authorized applicant within the issuance domain. Authentication shall rely upon certificates issued under Swedish Public Sector Internal Root CA v1 to individuals with identity assurance level 3.

3.2.6. Criteria for interoperation

Inter-operation is not allowed.

3.3. Identification and Authentication for Re-Key Requests

Re-keying is not allowed.

3.3.1. Identification and authentication for routine re-key

No stipulation.

3.3.2. Identification and authentication for re-key after revocation

No stipulation.

3.4. Identification and Authentication for Revocation Request

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

- The certificate subscriber
- An id-administrator or authorized applicant within the issuance domain
- The applicable processing centre
- The EFOS Operational Authority

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

Acceptable procedures for authenticating the revocation requests of a subscriber are as follows:

Revocation request from	Method for revocation	Identification method
	Self-administration portal	Authentication by mutual TLS with a certificate issued by a CA that is trusted by EFOS or EOOBAS.

Subscriber	Telephone call	Call to the support center that asks control questions (for card number, personal id) that proves that the caller has knowledge about the certificate to be revoked.
Id-administrator, authorized applicant or other authorized representative within issuance domain	Administration portal	Authentication by mutual TLS with a certificate issued by EFOS where the identity assurance level is 3 or EOOBAS.
	Telephone call	Call to the support center that asks control questions (for card number, personal id) that proves that the caller has knowledge about the certificate to be revoked.
Person within EFOS operational authority	Administration portal	Authentication by mutual TLS with a certificate issued by EFOS where the identity assurance level is 3.
	Telephone call	Call to the EFOS technical operations that asks control questions (for card number, personal id) that proves that the caller has knowledge about the certificate to be revoked.
Processing centre	API	Revokes certificates in case of production errors.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

Below is a list of entities that may submit certificate applications:

- Individual who is the subject of the certificate and who is an employee of, or has a professional correlation with, an organization within the issuance domain
- Authorized representatives of an organization within the issuance domain
- Id-administrators or authorized applicants within an issuance domain
- Persons within the EFOS operational authority

4.1.2. Enrollment Process and Responsibilities

Id-administrators and authorized applicants within the issuance domain have the utmost responsibility in validating the application itself as well as the identity of the individual or function. All validations shall be done in accordance with the EFOS issuance routines and the EFOS trust framework, prior to authorizing issuance of a certificate.

For functions EFOS validation specialists are responsible for managing the function rulesets for each issuance domain. The function rulesets control the scope of allowed certificate subject names for id-administrators and authorized applicants.

Each Applicant shall submit sufficient information and documentation for the EFOS PKI or the issuance domain to perform the required verification of identity prior to issuing a Certificate.

All communication during the Certificate Application process, including delivery of public keys to be included in Certificates, shall be authenticated and protected from modification.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

An id-administrator or authorized applicant shall perform identification and authentication of all required subscriber information according to the requirements in chapter 3. Identification and authentication shall be done in accordance

with EFOS issuance routines and the EFOS trust framework and may vary depending on the type of certificate being issued.

The id-administrator or authorized applicant signs the application ensuring that all requirements regarding application processing have been fulfilled.

4.2.2. Approval or Rejection of Certificate Applications

An id-administrator or authorized applicant will approve an application for a certificate if any of following criteria are met:

- The certificate application can be verified in accordance with chapter 3

An id-administrator or authorized applicant will reject an application for a certificate if the following criteria are met:

- The certificate application cannot be verified in accordance with chapter 3 shall be rejected.
- The applicant fails to provide supporting documentation upon request
- The applicant fails to respond to notices within a specified time
- The id-administrator or authorized applicant suspects that the applicant may have malicious intent.

4.2.3. Time to Process Certificate Application

CAs and id-administrators shall begin processing certificate applications within a reasonable time. There is no stipulation as to the completion time for an application.

A certificate application remains active until rejected.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

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

Certificates are generated when a member of the EFOS operational authority, id-administrator or authorized applicant has ascertained that all application and control routines have been fulfilled.

Every certificate application from a member of the EFOS operational authority, id-administrator or authorized applicant can be traced back to the individual that signed the certificate application.

During the certificate issuance process, the EFOS PKI shall verify that the information regarding the individual is up to date with the Tax Agency when applicable.

4.3.2. Notification to Subject by the CA of Issuance of Certificate

The EFOS PKI shall notify subscribers upon the creation of certificates that are associated certificates are made available to end entity subscribers allowing them to view, download or revoke them by means of selfservice.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

For functions:

- Failure of and authorized applicant to object to a certificate within 2 business days constitutes the subscribers acceptance of the certificate.

For RPAs:

- Signing a receipt for an RPA id for robots/RPA with a certificate, constitutes the subscribers acceptance of the certificate

For individuals:

- Signing a receipt for an EFOS E-id for individuals with a certificate, constitutes the subscribers acceptance of the certificate.

Failure of the subscriber to object to the certificate or its content constitutes certificate acceptance.

A period of two business days after the retrieval of the certificate by the Subject, or use of the certificate by the Subject, constitutes the Subject’s acceptance of the certificate.

4.4.2. Publication of the Certificate by the CA

All certificates issued by the EFOS PKI shall be published in the EFOS CAs database.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No notifications are sent to other entities.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Use of the private key corresponding to the public key in the certificate shall only be permitted once the subscriber has agreed to the subscriber agreement and accepted the certificate. The certificate shall only be used in accordance with:

For individuals:

- The EFOS E-id terms and conditions

For RPAs:

- The RPA E-id terms and conditions

For functions:

- The EFOS function terms and conditions

Certificate use must be consistent with the KeyUsage field extensions included in the certificate.

Certificate usage must only be used for their intended purpose according to below:

- Individuals eg. users – Authentication and signing certificates to smart cards/or equal and mobile devices intended to identify physical persons
- RPA - Authentication and signing certificates to smart cards or soft cert intended to identify RPA/robots
- Function – TLS/signing certificates for machines, servers and shared email addresses intended to identify/signing non-human entities

Subscribers shall discontinue use of the private key following expiration or revocation. Subscriber shall also protect their private keys from unauthorized use.

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties, that are not part of an issuance domain, and wish to use EOOBAS, must sign an additional agreement designed for this purpose.

Relying parties that use EFOS certificates to identify subscribers shall independently ensure:

- That certificates are only used to verify the identity of subscribers in accordance with this CP. EFOS and its issuance domains are not responsible for assessing the appropriateness of the use of a certificate.
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate.
- Relying parties are responsible for only allowing certificates to be used according to their intended purpose as stated below:
    - Individuals eg. users – Authentication and signing certificates to smart cards/or equal and mobile devices intended to identify physical persons
    - RPA - Authentication and signing certificates to smart cards or soft cert intended to identify RPA/robots
    - Function – TLS/signing certificates for machines, servers and shared email addresses intended to identify non- human entities
- That the status of the certificate, and all the CAs in the chain that issued the certificate, are valid and not revoked. For EOOBAS, however, this control is ensured by the EFOS PKI.
- Relying parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations in accordance with RFC5280, X.509 and applicable IETF PKIX standards. Such operations include verifying the validity of each certificate relied upon, identifying a certificate chain and verifying the digital signatures on all certificates in the certificate chain.

4.6. Certificate Renewal

4.6.1. Circumstance for Certificate Renewal

Certificate renewals are conducted in the same manner as new certificate applications.

4.6.2. Who May Request Renewal

Renewal is not allowed

4.6.3. Processing Certificate Renewal Requests

Renewal is not allowed

4.6.4. Notification of New Certificate Issuance to Subscriber

Renewal is not allowed

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewal is not allowed

4.6.6. Publication of the Renewal Certificate by the CA

Renewal is not allowed

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

Renewal is not allowed

4.7. Certificate Re-Key

Certificate re-keying is not allowed

4.7.1. Circumstance for Certificate Re-key

Certificate re-keying is not allowed

4.7.2. Who May Request Certificate Re-key

Certificate re-keying is not allowed

4.7.3. Processing Certificate Re-key Requests

Certificate re-keying is not allowed

4.7.4. Notification of Certificate Re-key to Subject

Certificate re-keying is not allowed

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

Certificate re-keying is not allowed

4.7.6. Publication of the Issued Certificate by the CA

Certificate re-keying is not allowed

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

Certificate re-keying is not allowed

4.8. Certificate Modification

Certificate modifications are conducted in the same manner as new certificate applications.

4.8.1. Circumstance for Certificate Modification

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CP. The new certificate may have the same or a different subject public key. Additional examples of circumstances when certificate modification may occur include minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures, organizational name change (e.g. as the result of merger, acquisition, or legally documented name change), and the replacement of the certificate where a minor error in certificate information or profile has been discovered.

After modifying a client certificate, the EFOS PKI may revoke the old certificate but may not further re-key, renew, or modify the old certificate.

4.8.2. Who May Request Certificate Modification

The EFOS PKI may modify certificates at the request of the Subject or at its own discretion.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, the EFOS PKI shall verify any information that will change in the modified certificate. The EFOS PKI shall issue the modified certificate only after completing the verification process on all modified information. The validity period of a modified certificate shall not extend beyond the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4. Notification of new certificate issuance to subscriber

See 4.3.2, in the context of a certificate modification.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

See 4.4.1, in the context of a certificate modification.

4.8.6. Publication of the Modified Certificate by the CA

See 4.4.2.

4.8.7. Notification of certificate issuance by the CA to other entities

No stipulation.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Prior to revoking a certificate, the EFOS PKI shall verify that the revocation request was made in accordance with 3.4. The EFOS PKI shall revoke any certification the occurrence of any of the following circumstances:

- If the unique identity, eg. Subject serial number and names for individuals, of the subscriber whose information contained within certificate is changed
- If receiving a revocation request according to section 3.4 in this CP
- If the subject fails to retrieve the certificate within reasonable time of its availability
- If the original Certificate Request was not authorized
- If suspecting that a private key associated with a certificate is compromised or used by some entity that is not the subscriber
- If suspecting that the smart card or equivalent cryptographic module that contains the private key is no longer in use, or possessed, by the subscriber
- If suspecting that the subscriber violates the stipulations in the EFOS E-id terms and conditions
- If suspecting that the subscriber violates the stipulations in the EFOS function terms and conditions
- If EFOS PKI detects or otherwise becomes aware that the certificate or the subscriber is involved for malicious activities
- If the EFOS PKI detects or otherwise becomes aware that the Subscriber has lost its rights to a Domain Name or Organizational information contained within the certificate and fails to provide proof of company merger or otherwise
- If a Subject has been added as a denied entity, or has applied to be added, to the EFOS blacklist
- If EFOS PKI detects or otherwise becomes aware that a court has revoked a Subscriber's right to use the Domain Name or Organizational information contained within the certificate.
- If EFOS PKI detects or otherwise becomes aware of a material change in the information contained in the Certificate or that such information is no longer accurate or representative of the facts.
- If an error in production occurs within a processing centre.
- If an accountable issuer terminates its relationship with EFOS the EFOS PKI shall revoke all certificates issued in its issuance domain. This does not apply if the issuance domain signs an agreement for business transition to another issuance domain that inherit the responsibilities of the withdrawing accountable issuer.
- If a used CA-key is suspected of compromise
- If a CA ends its duties as a CA
- In such additional events that the EFOS Policy Authority determines, at its sole discretion, warrant revocation.

4.9.2. Who Can Request Revocation

Revocation requests can be made by:

- The certificate subscriber
- An id-administrator or authorized applicant within the issuance domain
- The applicable processing centre
- The EFOS Operational Authority

4.9.3. Procedure for Revocation Request

Entities submitting certificate revocation requests shall be identified according to 3.4

Accountable issuers are required to promptly revoke certificates involved in a security incident.

The EFOS PKI shall:

- Revoke a certificate within reasonable time if the request is authenticated in accordance with 3.4.
- Provide a 24/7/365 response to any certificate security incident reports.
- List revoked certificates in applicable CRL and OCSP services where they shall be published until one full publication cycle after the end of the certificate's validity.
- Publicly disclose its revocation and incident reporting procedures.

Initiations of a revocation request to the CA must be signed by an authorized individual or be performed with multi-person control.

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

4.9.4. Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible but still within a reasonable time.

4.9.5. Time within which CA Must Process the Revocation Request

Revoked certificates are published in the latest revocation list within one hour after a certificate is marked for revocation. The decision to revoke a certificate is normally done in relation to receiving the revocation request.

4.9.6. Revocation Checking Requirement for Relying Parties

It is solely the responsibility of relying parties to verify certificates revocation and suspension status in accordance with this CP before a certificate is used.

Relying parties shall verify revocation status through CRLs or OCSPs identified in each certificate in the chain.

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

- The revocation control is made against a current revocation list
- The revocation list is still valid
- The digital signature of the revocation list is valid

However for EOOBAS revocation status is checked by EFOS and it is therefore not necessary for relying parties to repeat those checks.

4.9.7. CRL Issuance Frequency

EFOS CAs that issue end-entity certificates new CRLs will be issued at least every 30 minutes all days of the year.

FunctionCA	The EFOS CA CRL shall be updated and issued at least once every seven (7) days and record the date and time of the transaction in the CRL's Effective date field. The CRL's NextUpdate field value identifies the point in time when the CRL expires and MUST NOT be more than 7 days and 12 hours after the value of the Effective date field.
Other CAs	The EFOS CA CRL shall be updated and issued at least once every 72 hours and record

	the date and time of the transaction in the CRL's Effective date field. The CRL's NextUpdate field value identifies the point in time when the CRL expires and MUST NOT be more than 24 hours after the value of the Effective date field. Upon expiration of certain CAs a final CRL MAY be published that has a NextUpdate value that exceeds the time parameters noted elsewhere in this section.

EFOS Root CA is maintained in an offline state and will issue a new CRL at least once per year or whenever a CA certificate is revoked. Root CA CRLs shall have its nextUpdate attribute set to maximum 1 year after the issuance of the CRL.

Certificates that have expired may be removed from later issued CRLs.

4.9.8. Maximum Latency for CRLs

The publication to the CRL repositories shall not occur more than 30 minutes after CRL issuance.

4.9.9. On-line Revocation/Status Checking Availability

EFOS offers an on-line revocation/status checking service, OCSP.

OCSP services for issuing CAs shall be updated with the latest revocation information at least once every 60 minutes all days of the year

OCSP services for Root CAs shall be updated with the latest revocation information every time a new CRL is issued.

4.9.10. On-line Revocation Checking Requirements

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

This does however not apply to EOOBAS.

4.9.11. Other Forms of Revocation Advertisements Available

No other forms of revocation advertisements are available at present

4.9.12. Special Requirements Related to Key Compromise

Accountable issuers are required to report certificate security incidents according to the EFOS certificate security incident routine.

EFOS shall use reasonable efforts to notify potential Relying Parties upon the discovery or suspicion that its Private Key has been compromised and therefore has been or is to be revoked.

4.9.13. Circumstances for Suspension

Certificate suspension is not allowed in EFOS at present

4.9.14. Who Can Request Suspension

Certificate suspension is not allowed in EFOS at present

4.9.15. Procedure for Suspension Request

Certificate suspension is not allowed in EFOS at present

4.9.16. Limits on Suspension Period

Certificate suspension is not allowed in EFOS at present

4.10. Certificate Status Services

4.10.1. Operational Characteristics

EFOS shall make certificate status information available through CRL according to 4.9.7 and 4.9.8. EFOS will also make certificate status information available through OCSP according to 4.9.9 and 4.9.10.

4.10.2. Service Availability

EFOS shall provide certificate status services 24x7 without interruption excluding scheduled interruptions.

4.10.3. Optional Features

Certificates that have expired may be removed from certificate status services.

4.11. End of Subscription

Subscribers may end their subscription to certificate services either by:

- Requesting that their certificate(s) be revoked or;
- by allowing the certificate(s) to expire

4.12. Key Escrow and Recovery

End-entity Private Keys shall never be escrowed by EFOS.

4.12.1. Key Escrow and Recovery Policy Practices

No stipulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

5.1.1. Site Location and Construction

EFOS shall perform its CA operations from a secure data centre equipped with logical and physical controls that make the CA operations inaccessible to non-trusted personnel. The site location and construction, when combined with other physical security protection mechanisms such as guards, door locks, and intrusion sensors, shall provide robust protection against unauthorized access to the CA system, services, documentation and records.

The facilities that host a CA must also employ active surveillance and alarms that are monitored by guards 24 hours every day of the year.

CAs shall describe their site location and construction in more detail in their CPS.

5.1.2. Physical Access

Physical access requirements for accountable issuers and their issuance domains are described and agreed upon in the EFOS membership agreement and the EFOS trust framework.

EFOS shall protect its system components (computers, rooms, services, documentation, records, etc.) from unauthorized access and shall implement physical controls to reduce the risk of equipment being tampered with. EFOS shall store all removable media and paper containing sensitive plain-text information related to CA operations in secure containers. The security mechanisms should correspond to the level of threat to the equipment and data.

Activation data must either be memorized or recorded and stored in a manner that corresponds to the security afforded the cryptographic module and must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA equipment or private keys.

EFOS shall:

- Manually or electronically monitor its systems for unauthorized access at all times
- Maintain an access log that is inspected periodically
- Ensure that each EFOS CA deactivates, removes, and securely stores its CA equipment when not in

use. If the facility housing EFOS CA equipment is ever left unattended, the EFOS OA shall verify that:

- the CA is left in a mode of operation appropriate to its unattended state;
- all security containers are properly secured;
- physical security systems (e.g., door locks, vent covers) are functioning properly and are activated; and
- the area is secured against unauthorized access.

EFOS Policy Authority shall assign the explicit responsibility for making security checks to a person or group of persons. The person or persons within this group are assigned the trusted role EFOS internal auditor and shall maintain a log that identifies who performed the security check. Whenever the facility is left unattended, the last person to depart shall sign a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3. Power and Air Conditioning

EFOS shall ensure a back-up power supply and sufficient environmental controls to protect the CA systems. The protection must be sufficient for the CA to be able to automatically complete pending operations and record the system state prior to a shutdown caused by lack of power or an environmental conditioning error.

5.1.4. Water Exposure

EFOS shall protect its CA equipment from water exposure.

5.1.5. Fire Prevention and Protection

EFOS shall protect its CA equipment from fire by installing mechanisms which detect fire and act to suppress it.

5.1.6. Media Storage

Media storage requirements for accountable issuers and their issuance domains are described and agreed upon in the EFOS membership agreement and the EFOS trust framework.

EFOS shall protect all media from accidental damage and unauthorized physical access. EFOS shall duplicate and store its audit and archive information in a back-up location that is physically separate from its primary operations facility.

5.1.7. Waste Disposal

When needed EFOS shall destroy all data (electronic and paper) in accordance with [DoD5220.22M] procedures for permanently destroying such data.

5.1.8. Off-site Backup

EFOS shall ensure weekly system back-ups sufficient to enable recovery from system failure and shall store the backups, including at least one full backup copy, at an offsite location. The offsite location shall have procedural and physical controls that correspond to the backups operational location and which that the levels of control implied elsewhere in this CP.

5.2. Procedural Controls

5.2.1. Trusted Roles

EFOS personnel acting in Trusted Roles include system administration personnel and some of the personnel involved with subscriber, support and audit. EFOS shall design, document and publish the functions and duties performed by persons in Trusted Roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI. All personnel in Trusted Roles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations. EFOS PKI or the issuance domain shall be responsible for appointing individuals to Trusted Roles.

5.2.1.1. EFOS Operational Authority Manager

EFOS operational authority manager is the person utterly responsible for the group EFOS Operational

Authority. This is an administrative role responsible for the daily operations of the EFOS PKI.

5.2.1.2. EFOS Internal Auditor

EFOS internal auditor is a member of the EFOS operational authority, has the system role “read” for all issuance domains.

This is an administrative role whose responsibility includes but is not limited to:

- Reviewing, maintaining and archiving audit logs
- Performing and/or ensuring internal and external compliance audits to determine whether the EFOS personnel are operating in accordance with this CP.

5.2.1.3. EFOS External Auditor

An additional role external to EFOS CA is the External Auditor role, performed by an external auditor in accordance with Section 8.

5.2.1.4. EFOS administrative operator

Member of the EFOS Operational Authority, has the system role “EFOS Förvaltningsansvarig”. Is responsible for the configuration of issuance domains on a day to day basis. This includes but is not limited to:

- Delegated mandate to administer changes of trusted roles within established issuance domains
- Administering relationships between organizations within an issuance domain
- Assigning the role accountable issuer within an issuance domain on request from the EFOS policy authority
- Administering receipt and notification templates common to all issuance domains
- Administering offices for delivery of security tokens for all issuance domains
- Read and revocation rights within all issuance domains.

5.2.1.5. EFOS validation specialist

Member of the EFOS Operational Authority. Has the system role “EFOS valideringsspecialist”.

Is responsible for the verification, approval or denial of requests regarding rulesets for issuance of EFOS Function Certificates.

5.2.1.6. EFOS PKI Administrator

Member of the EFOS Operational Authority. Has the appropriate infrastructural roles in the CA system and on the server operating the CA system.

Is responsible for the maintenance of the CA system and the server operating the CA system. This responsibility includes but is not limited to:

- The installation, configuration and maintenance of EFOS CA software
- Administering CA accounts
- HSM maintenance and key generation
- Key back-up and key management.
- Performing and securely storing regular system back-ups of the EFOS CA system.
- Performing restoration checks for the EFOS CA software and keys according to the EFOS continuity

plan Is subject to restrictions regarding number of persons required per task according to 5.2.2.

5.2.1.7. EFOS System Administrator/ System Engineer (Operator)

Member of the EFOS Operational Authority. Has the appropriate infrastructural roles on the server operating the CA system, network equipment and database servers.

Is responsible for the maintenance of the CA system and the server operating the CA system. This responsibility includes but is not limited to:

- Administration and maintenance of EFOS-portal application servers
- Administration and maintenance of the PKI repositories listed in 2.1
- Administration and maintenance of EFOS-portal database servers
- Administration and maintenance of routers, firewalls, and network configurations.
- Ensuring that systems are updated with software patches

- Performing regular backups of the EFOS database and the EFOS-portal application an configuration
- Performing restoration checks for the EFOS data base and EFOS-portal according to the EFOS continuity plan
- Other maintenance needed to ensure system stability and recoverability.

Is subject to restrictions regarding number of persons required per task according to 5.2.2.

5.2.1.8. EFOS technical administrator

Member of the EFOS Operational Authority. Has the system role “EFOS Portaladministratör”

Is responsibility managing the technical configuration of EFOS-portal on a daily basis. This includes but is not limited to:

- Configuration of certificate and token templates
- Monitoring and maintaining connections to external dependencies
- Creating new organizations

Is subject to restrictions regarding number of persons required per task according to 5.2.2.

5.2.1.9. Accountable issuer

An administrator within an issuance domain and the person utmost responsible for issuance of certificates. Has the role “Ansvarig utgivare”. This is not a role in EFOS-portal.

5.2.1.10. Issuance domain id-administrator

A group of different roles with rights in a hierarchical structure. One ore sometimes more of these roles are assigned to persons within an issuance domain. Persons with one of these roles are responsible for the issuance of certificates to subscribers on a day to day basis.

Depending on the exact role the responsibility may consist of but is not limited to:

- Requesting the issuance and revocation of certificates for Subscribers.
- Conducting identity verification upon issuance and/or extradition of certificates
- Compliance with required issuance and revocation steps according to established instructions

5.2.2. Number of Persons Required per Task

At least the following tasks shall only be allowed to be performed with (n out of m) multi-person control:

- Access to the CA-vault where HSM, CA software, Private keys and related material are operated or stored
- Access to CA software and CA private key backups
- During migration of CA private keys between security modules access to encrypted CA private keys, activation data and private keys used for the encryption shall be separated between multiple persons.
- Access to personalized, but not delivered, end-entity cryptographic modules stored within Processing centre
- Access to subscriber activation data during generation at Processing centre

At least the following tasks shall only be allowed to be performed if the user has been identified with strong authentication and identity assurance level 3 or with (n out of m) multi-person control:

- Access to and administration of Application servers for EFOS-portal
- Access to and administration of Database servers for EFOS-portal
- Access to and administration of EFOS PKI repository servers
- Access to and administration of EFOS infrastructural operation components, for example network devices.
- Access to and administration of EFOS declaration of assurance
- Issuance of certificates by means of EFOS-portal

5.2.3. Identification and Authentication for each Role

Access rights to all systems within EFOS shall only be granted if users have undergone strong authentication with identity assurance level 3.

Central systems involved in the operations of EFOS may allow access with a lower grade of authentication but only if

(n out of m) multi-person control is applied.

5.2.4. Roles Requiring Separation of Duties

- The EFOS operational authority manager shall serve to fulfil the requirement of multi-party control for physical access to the CA-vault, but may not have logical access rights to any of the system within the vault. This role may not be assigned any roles that independently can issue certificates to other subscribers
- An EFOS internal auditor shall serve to fulfil the requirement of multi-party control for physical access to the CA-vault, but may not have logical access rights to any of the system within the vault. The EFOS internal auditor role may only have the system role “Läs” and shall not have any other rights than read access to logs, documents and similar.
- An EFOS administrative operator shall not be assigned the roles:
    - EFOS technical administrator
    - EFOS system administrator
    - EFOS id-administrator
- A EFOS validation specialist shall not be assigned the roles:
    - EFOS technical administrator
    - EFOS system administrator
    - EFOS id-administrator
- A EFOS PKI Administrator shall not be allowed to assume the role of EFOS internal auditor
- A EFOS System Administrator shall not be allowed to assume the role of EFOS internal auditor
- EFOS Technical Administrator shall not be allowed to assume the roles:
    - Internal auditor
    - Validation specialist
    - EFOS id-administrator

Separation of duties may be enforced either by EFOS-portal, the CA equipment, or procedurally, or by both means. No individual shall have more than one identity.

There shall be the means to audit adherence to these rules.

5.3. Personnel Controls

The EFOS Policy Authority has documented detailed personnel control and security policies for EFOS and accountable issuers to adhere to and be audited against.

All persons that hold a trusted role shall, beyond personnel controls, also be properly identified.

A selection of the listed personnel controls must be applied to both the EFOS PKI personnel and for the accountable issuer for each issuance domain. Proof of performed personnel controls shall be documented and provided to the EFOS Policy Authority upon demand.

Accountable issuers shall describe which personnel controls are performed on id-administrators within their issuance domain in the declaration of assurance. For other personnel within the issuance domain the same procedures are recommended but optional.

Personnel controls and documentation of proof shall only be gathered in adherence to applicable laws and local policies.

5.3.1. Qualifications, Experience, and Clearance Requirements

The EFOS PKI and accountable issuers shall require that personnel seeking to become trusted persons present proof of trustworthiness, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Personnel involved in time-stamping operations must possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures.

5.3.2. Background Check Procedures

The EFOS PKI and accountable issuers shall conduct background checks for personnel seeking to become trusted persons.

Background checks for these persons shall be repeated periodically as part of the EFOS revision plan.

Background check for trusted roles shall include security controls performed by a trusted Swedish authority.

Background checks for accountable issuers, accountable issuer security responsible and id-administrator acknowledged by EFOS are according to EFOS trust framework.

Reports from background checks shall be evaluated and result in actions that are reasonable compared to the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for trusted positions or the termination of existing trusted persons.

5.3.3. Training Requirements

EFOS will enable requisite training to all personnel with a Trusted Role.

Training should be started or completed before the person may assume his or her duties.

EFOS shall maintain records of who received training and what level of training was completed for all trusted roles except id-administrators and security responsible persons within the accountable issuers. Accountable issuers are responsible for ensuring that id-administrators in their issuance domain have received training and have the knowledge and ability to perform duties according to their role.

All training materials shall be periodically reviewed and address the elements relevant to functions performed by the personnel.

The training relates to the person's job functions and covers but is not limited to:

- Security principles and mechanisms of EFOS
- basic Public Key Infrastructure (PKI) knowledge;
- administration and knowledge of hardware and software versions used by the EFOS PKI;
- ITIL process handling within EFOS
- disaster recovery and business continuity procedures;
- common threats to the validation process, including phishing and other social engineering tactics, and [CABF].
- All duties the person is expected to perform
- Knowledge of EFOS routines and policies
- Incident and compromise reporting and handling
- Authentication, identification and verification routines and policies
- Validation of ownership for functions

5.3.4. Retraining Frequency and Requirements

EFOS personnel shall maintain skill levels that are consistent with industry-relevant training in order to continue acting in Trusted Roles.

EFOS and accountable issuers shall ensure that personnel acting in Trusted Roles:

- have knowledge and ability to perform duties according to their role over time.
- are made aware of any changes to the changes in policies and routines.

EFOS policy authority may enforce retraining requirements upon major changes in routines and policies.

5.3.5. Job Rotation Frequency and Sequence

No stipulations

5.3.6. Sanctions for Unauthorized Actions

EFOS and accountable issuers shall ensure appropriate administrative and disciplinary actions are taken against

personnel who violate this policy.

5.3.7. Independent Contractor Requirements

EFOS and accountable issuers may permit independent contractors or consultants to become trusted persons only to the extent necessary to accommodate clearly defined outsourcing relationships and only under the following conditions:

- The entity using the independent contractors or consultants as trusted persons does not have suitable employees available to fill the roles of trusted persons, and
- The contractors or consultants are trusted by the entity to the same extent as if they were employees.

Otherwise, independent contractors and consultants shall have access to secure facilities used within EFOS only to the extent they are escorted and directly supervised by trusted persons.

5.3.8. Documentation Supplied to Personnel

EFOS and accountable issuers shall provide personnel in Trusted Roles with documentation or tools necessary to perform their duties.

5.4. Audit Logging Procedures

Audit logs shall be reviewed both periodically and in response to alerts based on irregularities and incidents within EFOS systems.

Automated tools may be used to scan for anomalies or specific conditions.

Audit log processing shall consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. During processing a statistically significant set of security audit data generated since the last review and make a reasonable search for any evidence of malicious activity.

Audit log reviews shall include a verification that the log has not been tampered with.

Actions taken based on audit log reviews shall be documented.

Processing centre shall compare their audit logs with the supporting manual and electronic logs from EFOS and accountable issuers when any action is deemed suspicious.

5.4.1. Types of Events Recorded

The types of auditable events that must be recorded by EFOS and/or accountable issuers are set forth below. All logs, whether electronic or manual shall contain:

- the date and time of the event traceable to UTC (SP)
- the identity of the entity that caused the event
- the identity of the affected entity
- type of the affected entity
- if the operation was successful or failed

CAs shall state the logs and types of events they record in their CPS.

Types of auditable events include:

- Operational events (including but not limited to (1) the generation of CAs own keys and the keys of subordinate CAs, (2) start-up and shutdown of systems and applications, (3) changes to CA details or keys,(4) cryptographic module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement), (5) possession of activation data for CA private key operations, physical access logs, (6) system configuration changes and maintenance, (7) Records of the destruction of media containing key material, activation data, or personal subscriber information)
- Certificate lifecycle events (including but not limited to initial issuance, renew, revocation)
- Trusted employee events (including but not limited to (1) logon and logoff attempts, (2) attempts to create, remove, set passwords or change the system privileges of the privileged users, (3) personnel changes)

- Discrepancy and compromise reports (including but not limited to unauthorized system and network logon attempts)
- Operations performed on EFOS repositories, servers and infrastructural components
- Changes to certificate creation policies and templates e.g., validity period and certificate content
- Ruleset and configuration events

If the event cannot be recorded automatically a manual procedure shall be implemented to satisfy the requirements.

All event records shall be made available to auditors upon request as proof of the EFOS and/or accountable issuers adherence to EFOS routines and policies.

5.4.2. Frequency of Processing Log

EFOS shall, at least every two months:

- review system and audit logs
- make system and file integrity checks

5.4.3. Retention Period for Audit Log

EFOS shall retain audit logs on-site until they have been reviewed.

After review audit logs may be archived according to 5.5.2

5.4.4. Protection of Audit Log

Audit logs shall be protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

Logs are protected from unauthorized access and modification by:

- Using logical protection mechanisms within the operating system or the application
- Making the systems physically and logically inaccessible for unauthorized persons
- Ensuring that access to logs are only given to authorized trusted persons
- Monitoring access to logs by all entities

Audit log access is reviewed and verified at least once every month.

EFOS shall implement procedures that protect archived data from destruction prior to the end of the audit log retention period.

EFOS may disclose audit logs to relevant parties, eg. Auditors, upon request and if not prohibited by applicable law.

5.4.5. Audit Log Backup Procedures

Incremental backups of audit logs shall be created daily and full backups are performed weekly. A copy of backups shall be stored off-site.

5.4.6. Audit Collection System (internal vs. external)

EFOS may use an EFOS internal and automated audit collection system.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

Vulnerability scans and penetrations tests shall be performed in accordance with guidelines from CA Browser Forum. Any findings are documented and prioritized on severity by those performing the test. EFOS Operational Authority later assesses and takes actions based on the report. The work is documented for future reference. Findings and actions taken shall be reported to the EFOS Policy Authority.

EFOS and accountable issuers shall perform risk assessments when needed, but at least annually. Risk assessments shall identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process.

EFOS shall perform risk assessments and maintain a Security Plan according to CA Browser Forum Baseline Requirements or equivalent. The Security plan shall be updated when needed, but at least annually.

5.5. Records Archival

5.5.1. Types of Records Archived

EFOS shall retain the following information in its archives:

- Current and previous versions of: Trust framework, CP, CPS, Certificate profiles, RPA, Terms and Conditions, Function Terms and Conditions
- Current version of: Declaration of assurance and EFOS membership agreements
- Results and measures taken to comply to audits of EFOS operations
- All current and previous: Public and private CA-key and related cryptographic module operations, at least, generation, access to, modification, export, import and destruction
- System and equipment configurations, modifications; and updates
- All transactions that contain signed requests for lifecycle management of certificates
- Issued and revoked certificates and related updates to certificate repositories
- Any documentation related to the receipt or acceptance of a certificate or token
- All security incidents, at least:
    a. Any attempt to delete or modify audit logs
    b. Violations of the CP or CPS
    c. Suspected and confirmed key compromise issues
    d. Actions taken as a result of violations of physical security
- Appointment of an individual to a Trusted Role

In cases when the archived information consists of digitally signed information, information that is required for signature verification is also archived.

EFOS may archive data manually or automatically. If automatic archival is implemented, EFOS shall synchronize its archived data on a daily basis.

5.5.2. Retention Period for Archive

EFOS shall retain archived data for at least 10 years from the time of data generation, unless a greater retention is required by any other applicable law or local policy.

Up to now and currently there is no culling of the archived information.

5.5.3. Protection of Archive

EFOS shall store its archived records at a secure off-site location in a manner that prevents unauthorized access, modification, substitution, or destruction.

If the original media cannot retain the data for the required period, the archive site must define a mechanism to periodically transfer the archived data to new media.

EFOS shall maintain any software application and a suitable software/hardware host system required to process the archive data until the data is either expired or then destroyed, or it is transferred to a newer medium.

5.5.4. Archive Backup Procedures

EFOS shall back up system archives incrementally on a daily basis and perform full backups on a weekly basis. Further description of archive backup procedures shall be described in the CPS.

5.5.5. Requirements for Time-stamping of Records

EFOS shall automatically time-stamp archive records as they are created, using a time-signal per §6.8. Cryptographic time-stamping of archive records is not required.

5.5.6. Archive Collection System (internal or external)

EFOS shall collect archive information internally.

5.5.7. Procedures to Obtain and Verify Archive Information

EFOS shall not release archives unless requested by the EFOS Policy Authority or as required by law. Only authorized trusted personnel are able to obtain access to the archive.

EFOS may allow subscribers and accountable issuers to obtain a copy of their own archived information. The integrity of information is verified when it is restored from archive.

5.6. Key Changeover

A CA certificate may be renewed upon approval from the EFOS Policy Authority.

Following an approval of a renewal request, EFOS shall conduct a key generation ceremony in order to generate a new key pair for the CA. Such key generation ceremony shall meet the key ceremony requirements documented by the CA/Browser Forum's Baseline Requirements. New CA certificates containing the new CA public keys generated during such key generation ceremony shall be made available to relying parties through PKI repositories and communicated by means of newsletters.

New CA keys are created at least 3 months before the existing CA key ceases to be used for signing issued certificates.

The EFOS PKI shall periodically change its Private Keys in a manner set forth in the CPS that prevents downtime in the EFOS PKI's operation. After key changeover, the EFOS PKI shall sign certificates using only the new key. The EFOS PKI shall still protect its old Private Keys and shall make the old Public Key Certificate available to verify signatures until all of the certificates signed with the old Private Key have expired.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

The EFOS PKI shall have redundant CA systems that are located at separate, geographically diverse locations and that are configured for automatic failover in the event of a disaster (Disaster Recovery/Mirror Site).

EFOS shall implement data back-up and recovery procedures and shall develop a Disaster Recovery and/or Business Continuity Plan (DR/BCP).

EFOS shall review, test, and update the DR/BCP and supporting procedures annually. If a disaster occurs, EFOS shall re- establish operational capabilities as quickly as possible.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

EFOS shall make regular back-up copies of its Private Keys and store them in a secure off-site location.

EFOS shall also make system back-ups on a daily basis.

If a disaster causes the EFOS PKI operations to become inoperative, EFOS shall, after ensuring the integrity of the CA systems, re-initiate its operations on replacement hardware located at a secure facility, using back-up copies of its software, data, and Private Keys.

EFOS shall give priority to re-establishing the generation of certificate status information and thereafter certificate revocation and issuance.

If the Private Keys are destroyed, the EFOS shall re-establish operations as quickly as possible, giving priority to generating new key pairs.

5.7.3. Entity Private Key Compromise Procedures

If EFOS suspects that a CA Private Key is comprised or lost then EFOS shall follow its Incident Response Plan and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action. If

necessary a CA certificate and the related private key may be revoked.

If there is a compromise or loss EFOS shall notify relying parties and accountable issuers and make information available that can be used to identify which certificates and time-stamp tokens affected, unless doing so would compromise the security of the Subscribers or the EFOS PKI services.

After a CA private key compromise EFOS personnel shall report the results of the investigation. The report must detail the cause of the compromise or loss and the measures that should be taken to prevent a re-occurrence.

Following revocation of an EFOS CA certificate and implementation of the EFOS Incident Response Plan, EFOS will generate a new CA Key Pair and sign a new CA certificate in accordance with its CPS. EFOS shall distribute the CA-certificate in accordance with Section 6.1.4.

5.7.4. Business Continuity Capabilities after a Disaster

EFOS shall establish a secure facility in at least one secondary location, to ensure that all components remain operational in the event of a disaster at the EFOS PKI main site.

EFOS shall also continually verify backup restore procedures for all components to prepared for the event that all sites suffer a disaster.

5.8. CA or RA Termination

If an accountable issuer is terminated from EFOS, the accountable issuer is obligated to perform the termination in accordance with the EFOS trust framework.

In the event a CA is terminated from EFOS, EFOS is obligated to fulfil the following procedures:

- Inform subscribers and other parties that the CA has a relation with regarding the conditions for the termination, at least three months before termination
- Publicly inform relying parties and EFOS accountable issuers regarding the conditions for the termination, at least three months before termination
- Upon a CAs termination cease with issuance and remove functions for:
    a. revocation lists
    b. OCSP
    c. publication of chain certificates that are related to the CA whose keys are terminated. This also means that current revocation lists are removed from their repositories and that no new revocation lists are published as replacements.
- Terminate all permissions that are held by subcontractors in regards to a CA that is targeted for termination
- Ensure that all archived information and logs are kept for the entire duration of the archival period

A CA within EFOS must provide guarantees and insurances that the necessary means are available to fulfil the above requirements in a termination situation.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

EFOS shall generate and protect cryptographic keying material for CAs on a FIPS 140-2 level 3 validated cryptographic module using multiple individuals acting in Trusted Roles. When generating keying material, EFOS shall create auditable evidence to show that the EFOS PKI enforced role separation and followed its key generation process.

EFOS shall generate CA private keys based on random numbers that cannot be calculated regardless of what knowledge an entity might have regarding the circumstances for the key generation.

EFOS shall have an independent third party auditor validate the execution of the key process by either witnessing the key generation or by examining the signed and documented record of the key generation.

Subscriber private keys must be generated using a FIPS-approved method.

Generation of subscriber private keys for functions are either:

- If the method for issuing is PKCS#10 – Generated by the subscriber and beyond the control of EFOS
- If the method for issuing is PKCS#12 – Generated by the EFOS-

portal Generation subscriber private keys for persons must either be:

- Generated in the chip of a secure cryptographic module. These cryptographic modules shall be certified to at least NIST FIPS 140-2 level 2 or Common Criteria EAL4+ and use a random number generation according to NIST SP800-90A.
- For certificates issued from Swedish Public Sector Mobile ID CA v1, generated within a secure application delivered by EFOS. The secure application shall use a random number generation according to NISTSP800-90A

6.1.2. Private Key Delivery to Subscriber

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

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

To achieve identity assurance level 3 private keys shall either be generated by the subscriber or, if generated by a processing center, be delivered by means of a channel that is separated and secluded from the activation data. The channel must also be protected against manipulation.

Subscribers shall sign a receipt in connection to delivery of a private key. Before the receipt is signed the private key is not considered to be delivered and remain the in the responsibility of the entity holding it.

6.1.3. Public Key Delivery to Certificate Issuer

Public Keys shall be delivered to the EFOS PKI in a secure fashion and in a manner that binds the Subscriber's verified identity to the Public Key.

The certificate issuance shall ensure that the subscriber possesses the Private Key associated with the Public Key presented for certification.

6.1.4. CA Public Key Delivery to Relying Parties

EFOS shall provide its public keys to Relying Parties in a secure fashion and in a manner that prevents substitution attacks. EFOS will deliver its CA Public Keys to Relying Parties by means of:

a) The PKI repository

b) Authority Information Access links within a X.509 v3 certificate extension specified in the certificate.

6.1.5. Key Sizes

EFOS shall follow the NIST timelines in using and retiring signature algorithms and key sizes.

EFOS shall generate and use the following: keys, signature algorithms, and hash algorithms for signing end-entity certificates, CRLs, and certificate status responses:

a) 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256);

b) 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-512);

EFOS may require higher bit keys in its sole discretion.

Any certificates, whether CA or end-entity, expiring after 2030-12-31 must be at least 3072 bit for RSA and 521 bit for ECDSA.

6.1.6. Public Key Parameters Generation and Quality Checking

The EFOS PKI shall generate Public Key parameters for CAs and perform parameter quality checking in accordance with FIPS 140-2 level 3.

All CAs are required to keep up to date with developments and findings regarding cryptography and to adjust its algorithms in accordance with such developments and findings.

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

The EFOS PKI shall include key usage extension fields that specify the intended use of the certificate and technically limit the certificate's functionality in X.509v3 compliant software.

The EFOS PKI shall set key usage bits and assert extended key usage OIDs for each CA certificate in accordance with the EFOS CA certificate profile documents.

The EFOS PKI shall set key usage bits and assert extended key usage OIDs for each end-entity certificate type in accordance with the EFOS certificate profile documents.

6.2. Private Key Protection and Cryptographic Module Engineering Control

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

The responsibility for private key protection is divided as follows:

- CA private keys is the sole responsibility of the EFOS PKI
- End-entity cryptographic modules that are completed for delivery but are not yet sent to its recipient shall be locked in a controlled storage vault
- End-entity cryptographic modules that are ready for extradition but are not yet extradited to the subscriber are locked in a controlled storage vault within the issuance domain until it is extradited.
- Private keys for persons that are signed for by the subscriber is the sole responsibility of the subscriber
- Private keys for functions that are signed for by the id-administrator is the sole responsibility of the id-administrator

6.2.1. Cryptographic Module Standards and Controls

EFOS CAs shall use cryptographic modules validated to FIPS 140-2 level 3.

Subscriber private keys for functions should be stored, used and protected in a fashion that prevents key compromise and unauthorized access.

Subscriber private keys for persons must either be:

- Stored in the chip of a secure cryptographic module. These cryptographic modules shall be certified to at least NIST FIPS 140-2 level 2 or Common Criteria EAL4+.

- Certificates issued from Swedish Public Sector Mobile ID CA v1 will be stored within a secure application delivered by EFOS.

6.2.2. Private Key ('n' from 'm') Multi-person Control

See 5.2.2

6.2.3. Private Key Escrow

EFOS CAs shall not escrow its private keys.

6.2.4. Private Key Back-up

The EFOS PKI shall back-up its CA, CRL, and certificate status Private Keys. Security controls are implemented using multi-person control (n of m persons), se 5.2.2.

6.2.5. Private Key Archival

EFOS shall not archive CA or centrally generated subscriber Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All CA private keys must be generated by and in a cryptographic module.

EFOS shall only export its CA Private Keys from the cryptographic module to perform CA key back-up procedures or in case of a future migration to other cryptographic modules. Migration of private keys shall be performed according to applicable criteria within the WebTrust Principles and Critera for Certification Authorities.

When transported between cryptographic modules, EFOS shall encrypt CA private keys and protect the keys used for encryption according to 5.2.2.

6.2.7. Private Key Storage on Cryptographic Module

EFOS shall store its CA Private Keys on a cryptographic module which has been evaluated to at least FIPS 140-2 Level 3.

Subscriber private keys shall be stored according to 6.2.1

6.2.8. Method of Activating Private Key

EFOS shall activate its CA Private Keys in accordance with the specifications of the cryptographic module manufacturer.

For person certificates subscribers must authenticate themselves to the cryptographic module before activating their private keys. Entry of activation data shall be protected from disclosure.

For function certificates subscribers shall implement procedures to ensure that only the applicable function may activate the private key.

6.2.9. Method of Deactivating Private Key

EFOS shall deactivate its CA Private Keys and store its cryptographic modules in secure containers when not in use. EFOS shall prevent unauthorized access to any deactivated cryptographic modules.

Person certificate subscribers are responsible for deactivating their private keys when not in use. The private key may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. However deactivation of the private key is not equal to an actual logout from the system where the private key was used to gain access.

6.2.10. Method of Destroying Private Key

When required, CA private keys are destroyed in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. For hardware cryptographic modules storing EFOS CAs private keys, EFOS personnel with trusted roles may destroy the Private Keys by executing a "zeroize" command.

Physical destruction of hardware cryptographic modules for CA private keys is not required unless the cryptographic module has been compromised or is to be discarded.

Upon destruction of a CA private key EFOS shall ensure that the private key backups and its associated storage media is destroyed.

EFOS may destroy the subscriber Private Keys by overwriting the data upon request from the subscriber or and authorized id-administrator.

Accountable issuers are responsible to ensure that subscriber's private keys within their issuance domain are destroyed when the corresponding certificate is revoked or expired or if the Private Key is no longer needed.

6.2.11. Cryptographic Module Rating

See §6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

EFOS shall archive a copy of each issued certificate and the corresponding public key.

6.3.2. Certificate Operational Validity Periods and Key Pair Usage Validity Periods

EFOS certificates, including renewed certificates, have maximum validity periods of:

Type	Private Key Use	Certificate Term
Root CA	20 years	25 years
Sub CA	12 years	15 years
Subscriber Person Certificate	5 years	5 years
Subscriber Function Certificate	2 years	2 years

Upon the end of the usage period for a subscriber or CA key pair, the subscriber or CA shall thereafter cease all use of the key pair. However expired certificates may still be used to validate signatures generated before expiration and decrypt data encrypted before expiration.

EFOS may retire its CA Private Keys before the periods listed above to accommodate key changeover processes. EFOS shall not issue a Subscriber certificate with an expiration date that is past the signing CAs validity.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

EFOS shall generate activation data that has sufficient strength to protect its CA Private Keys. If a CA uses passwords as activation data for a signing key, EFOS CA shall change the activation data upon renewal of the CA certificate.

EFOS may only transmit activation data for CAs outside the CA-vault by means of a channel that is separated and secluded from the associated cryptographic module and according to 5.2.2. The channel must also be secured against manipulation.

When passwords are used as activation data for function certificates, subscribers shall generate passwords that cannot easily be guessed or cracked by for example dictionary attacks.

For person subscribers activation data is either:

- Generated by the processing center upon manufacturing the cryptographic module. Activation data (PIN/PUK-codes) shall be generated with good entropy and using multi-person control according 5.2.2
- Chosen by the subscriber as part of the certificate issuance process. Subscribers shall choose activation data with good entropy.

6.4.2. Activation Data Protection

EFOS CA shall protect activation data used to unlock CA private keys from disclosure using a combination of cryptographic and physical access control mechanisms achieving multi-person control according to 5.2.2.

EFOS shall require EFOS PKI personnel to memorize and not write down their password or share their passwords with other individuals. EFOS shall implement processes to temporarily lock access to secure CA processes if a specified number of failed log-in attempts occur.

Subscriber activation data (PIN/PUK-codes) for persons that is delivered from a processing center directly to the subscriber shall be protected in envelopes that are tamper proof and ensure that the codes are protected from unauthorized access.

During delivery from the processing center the activation codes are protected by using a delivery channel that is separated and secluded from the subscriber private keys. The channel must also be protected against manipulation.

Subscribers shall protect their activation data using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the corresponding private keys.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

EFOS shall configure its PKI systems, including any remote workstations used to access CAs and systems involved with PKI operations, to:

a) authenticate the identity of users before permitting access to the system or applications;

b) manage privileges of users to limit users to their assigned roles;

c) generate and archive audit records for all transactions;

d) enforce domain integrity boundaries for security critical processes; and

e) support recovery from key or system failure.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

For CAs, systems involved with PKI operations and workstations used to gain access to such systems, EFOS shall only use:

a) Software that was designed and developed under a formal and documented development methodology,

b) Approved hardware and software developed by verified personnel, using structured development approach and a controlled development environment,

c) Open source software that meets security requirements through software verification and validation and structured development/life-cycle management,

d) Hardware and software purchased and shipped in a fashion that reduces the likelihood of tampering, and

e) For CA operations, hardware and software that is dedicated only to performing the CA functions.

EFOS and its software suppliers shall implement procedures to prevent malicious software from being loaded onto CAs and systems involved with PKI operations. Such procedures shall include but is not limited to:

- Continuous code revisions during development
- Code revisions upon request from EFOS or independent auditors
- Startup and continuous hardware and software scans for malicious code
- Penetration tests on major changes and at least annually
- Continuously purchase or regularly develop updates to maintain security an functionality

- Using trusted and trained personnel to install the software and equipment.
- Not installing any software on its CAs and systems involved with PKI operations systems that are not part of the CAs operations.

EFOS shall use a formal configuration management methodology for installation and on-going maintenance.

Any modifications and upgrades shall be documented and controlled.

EFOS shall implement a mechanism for detecting unauthorized modifications to CAs and servers involved with PKI operations.

6.6.2. Security Management Controls

EFOS shall establish formal mechanisms to document, control, monitor, and maintain the installation and configuration of its CAs and systems involved with PKI operations, including any modifications or upgrades.

The Issuer CAs change control processes shall include procedures to detect unauthorized modification to the EFOS CAs systems and data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls.

When loading software onto a CA or a system involved with PKI operations system, EFOS shall verify that the software is the correct version and is supplied by the vendor free of any modifications.

EFOS shall verify the integrity of software used with its CA and systems involved with PKI operations at least once a week.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

EFOS shall document and control the installation, configurations and maintenance of network components involved with PKI operations, including any upgrades or modifications made.

EFOS shall implement a process for detecting unauthorized modifications to hardware or software for network components involved with PKI operations.

EFOS shall verify all software for network components, when first loaded, as the unmodified software.

EFOS shall implement appropriate network security controls, including turning off any unused network ports and services and only using network software that is necessary for the proper functioning of the CAs and systems involved with PKI operations.

6.8. Time-stamping

EFOS shall ensure that the accuracy of clocks used for time-stamping are synchronized and traceable to UTC

(SP). Electronic or manual procedures may be used to maintain system time.

Clock adjustments are auditable events.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

7.1.1. Version Number

The EFOS PKI shall issue X.509 version 3 certificates.

7.1.2. Certificate Extensions

The EFOS PKI shall

- Use certificate extensions in accordance with applicable industry standards, including RFC 5280.
- Document extensions in use and their criticality in the EFOS Certificate Profile
- Not issue certificates with a critical private extension.

7.1.3. Algorithm Object Identifiers

The EFOS PKI shall sign certificates using one of the following algorithms:

ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA1(1)}
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
SHA1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}

If the EFOS PKI signs certificates using RSA with PSS padding, the EFOS CA may use an RSA signature with PSS padding with the following algorithms and OIDs:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

The EFOS PKI and Subscribers may generate Key Pairs using the following:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }
id-keyExchangeAlgorithm	{ joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22 }

7.1.4. Name Forms

The EFOS PKI shall use distinguished names that are composed of standard attribute types, such as those identified in RFC 5280.

7.1.5. Name Constraints

EFOS may include name constraints in the `nameConstraints` field when appropriate.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The EFOS PKI shall use the OIDs listed in 1.2 and in the Figure 3 to identify its certificates and policies in the `certificatePolicies` extension.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

The EFOS PKI may include brief statements in the Policy Qualifier field of the `certificatePolicies` extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL Profile

7.2.1. Version number(s)

The EFOS PKI shall issue X.509 version 2 CRLs that conform to RFC5280.

7.2.2. CRL and CRL Entry Extensions

The EFOS PKI CRL extensions shall conform to the Extensions profile in RFC5280.

7.3. OCSP PROFILE

The EFOS PKI shall operate an OCSP service in accordance with RFC6960.

7.3.1. Version Number(s)

The EFOS shall support X.509 version 1 OCSP requests and responses.

7.3.2. OCSP Extensions

The EFOS PKI OCSP extensions shall conform to the Extensions profile in RFC6960

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or Circumstances of Assessment

On at least an annual basis, EFOS shall appoint one or more independent, third-party, auditors who shall assess its conformity with this CP.

EFOS CA shall have a program for compliance control.

EFOS shall have an audit program that covers audits on accountable issuers conducted by EFOS.

8.2. Identity/Qualifications of Assessor

For audits on EFOS conducted by an independent, third-party, auditor the requirements are at least one or more of the following:

- Licensed WebTrust Practitioner according to https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services
- Qualified auditor of the trust framework for Swedish e-ID and EFOS declaration of assurance to that

federation General requirements on personnel performing audits and other assessments:

- The scope of the audit or the assessment must be within the expertise of the personnel
- Must have a documented knowledge of the Swedish Public Sector, Identity Assurance practices and PKI standards and implementations.
- Must have a general knowledge of EFOS
- Must be trained and skilled in the auditing or assessment of secure information systems
- Must be familiar with organization compliance to trust frameworks, Information security management systems and IT, Internet and network security
- Must have a reputation for conducting its auditing and assessment business competently and correctly
- If a third-party is contracted the business must maintain Professional Liability/Errors and Omissions Insurance

8.3. Assessor's Relationship to Assessed Entity

EFOS shall utilize an independent auditor that has no financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the audited entity.

8.4. Topics covered by Assessment

Assessments by independent auditor's shall cover EFOS adherence to at least the following:

That EFOS and all issuance domains comply to the requirements of this CP and the EFOS trust framework.

That this CP and all certificates for persons issued under Swedish Public Sector Internal Root CA v1 are compliant to EFOS declaration of assurance towards the Swedish e-ID federation and the current version of the trust framework for Swedish e-ID's

That this CP and all certificates for functions issued under Swedish Public Sector Internal Root CA v1 are compliant to the current versions of the following external audit requirements. However as this PKI is a vital part in the infrastructure of the Swedish public sector some deviations may exist. These deviations will be documented.

- WebTrust Principles and Criteria for Certification Authorities, published at https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services
- CA Browser Forum Baseline Requirements, published at https://cabforum.org/for the Issuance and Management of Publicly-Trusted Certificates.

The EFOS Policy Authority shall continuously conduct audits to ensure compliance to the EFOS trust framework and this CP. The EFOS Policy Authority has the right to demand that accountable issuers take action on flaws found during audit in order to continue operating within EFOS.

8.5. Actions taken as a result of Deficiency

Deficiencies shall be dealt with according to the EFOS audit program published at EFOS.se

8.6. Communication of Results

A report of the results of each audit shall be delivered to the EFOS Policy Authority for review, approval and to decide upon recommended actions.

The results shall also be communicated to any entities entitled by law, regulation, or agreement to receive a copy of the audit results.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Any fees associated with the use of EFOS shall be regulated in the EFOS membership

agreement. Accountable issuers may set their own fees in their agreements with third parties.

9.1.1. Certificate issuance or renewal fees

According to 9.1

9.1.2. Certificate access fees

According to 9.1

9.1.3. Revocation or status information access fees

According to 9.1

9.1.4. Fees for other services

According to 9.1

9.1.5. Refund policy

According to 9.1

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Försäkringskassan shall maintain sufficient insurances in respect of its performance under this CP through Kammarkollegiet (The Legal, Financial and Administrative Services Agency) in accordance with ordinance on governmental agencies´ risk management (förordningen (1995:1300) om statliga myndigheters riskhantering).

9.2.2. Other Assets

Försäkringskassan processing centre and accountable issuers shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to subscribers and relying parties.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation

9.3. Confidentiality of Business Information

9.3.1. Scope of confidential information

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

9.3.2. Information not within the scope of confidential information

The following information is not considered as confidential:

- Issued certificates including associated public keys
- Revocation lists (CRL and OCSP)
- Relying Party Agreements
- Certification Practice Statements
- Certificate Policies

Exceptions can apply for information related to specific subscriber organizations if this is formally agreed upon between the EFOS Policy Authority and the subscriber organization.

9.3.3. Responsibility to protect confidential information

The EFOS personnel and contractors are responsible for protecting confidential information in accordance with the Offentlighets- och sekretesslag 2009:400 (Public Access to Information Act).

9.4. Privacy of Personal Information

9.4.1. Privacy plan

EFOS shall develop a privacy plan in accordance with the European general data protection regulation (EU) 2016/679, hence referred to as “Dataskyddsförordningen”.

CAs and processing centre shall implement a privacy policy that conforms to applicable local privacy laws. EFOS participants shall not disclose or sell the names of certificate applicants or other identifying information about them, subject to Section 9.3.2 and to the right of a terminating CA to transfer such information to a successor CA under Section 5.8.

All personnel involved with the EFOS PKI are expected to handle personnel information in strict confidence and meet the requirements of Swedish and European law concerning the protection of personal data. EFOS shall securely store and protect sensitive against accidental disclosure.

9.4.2. Information Treated as Private

Any information about subscribers that is not made available to a relying party through the subscriber's own use of the subscribers certificate is treated as private.

9.4.3. Information Not Deemed Private

Information disclosed through certificate status services are not considered private information.

9.4.4. Responsibility to Protect Private Information

EFOS PKI participants receiving private information shall secure it from compromise and disclosure to third parties and shall comply to applicable laws.

9.4.5. Notice and Consent to Use Private Information

Private information should not be used without giving notice to the party to whom that information applies. This section is subject to applicable laws.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7. Other Information Disclosure Circumstances

No other information disclosure shall be allowed within EFOS.

9.5. Intellectual Property Rights

Intellectual property rights are regulated in the EFOS membership agreement. Private

and public keys are the property of the Subscribers who rightfully hold them. EFOS

shall not knowingly violate the intellectual property rights of any third party.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

EFOS warrants that the EFOS PKI complies with this CP, the applicable CPS and all other stipulations referenced in these documents.

9.6.2. RA Representations and Warranties

Accountable issuers warrant that they comply to the requirements of this CP, the EFOS trust framework and the EFOS membership agreement.

9.6.3. Subscriber Representations and Warranties

Subscribers warrant to comply with the applicable of the following:

- EFOS electronic identity terms and conditions
- EFOS function terms and conditions

9.6.4. Relying Party Representations and Warranties

Relying Parties warrants to follow the procedures and requirements of this CP and in the applicable Relying Party Agreement prior to relying on or using a certificate issued by the EFOS PKI.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. Disclaimers of Warranties

EFOS disclaims all representations and warranties that are not explicitly mentioned in 9.6.2

9.8. Limitations of Liability

EFOS shall not be held liable if subscribers, relying parties or other entities use the EFOS PKI in contradiction with the EFOS terms and conditions of use for the Certificate, the applicable reyling party agreement, this CP and/or any other stipulations referenced in these documents.

9.9. Indemnities

Indemnities may be regulated in the EFOS membership agreements, the EFOS electronic identity terms and conditions and the EFOS function terms and conditions.

9.10. Term and Termination

9.10.1. Term

This CP and any amendments are effective according to the effective dates set forth in conjuction with the publication of the CP to the EFOS repositories, see 2.1. Each CP remains in effect until terminated or replaced with a newer version.

9.10.2. Termination

Prior to termination by deletion EFOS shall publish a notification no less than two (2) year (710 days) in advance.

If an affiliated organization fails to comply with the EFOS trust framework, EFOS shall notify the organization and provide the opportunity to fix the problem. If all attempts to agree, all valid certificates will be blocked and the service will be terminated for the organization.

9.10.3. Effect of Termination and Survival

Upon termination of this CP, EFOS participants and subscribers are still bound by the terms for each issued certificate for the remainder of the certificates validity period.

Responsibilities related to audit logs, archiving and the protection of confidential information will survive termination.

Upon termination EFOS may communicate additional conditions and effect's.

9.11. Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, EFOS participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

Notices are deemed effective after the sender and acknowledgment of receipt from EFOS.

9.12. Amendments

9.12.1. Procedure for Amendment

The EFOS Policy Authority determines what amendments should be made to this CP or the CPS. Controls are in place to ensure that this CP and the CPS is not amended and published without the prior authorization of the EFOS Policy Authority. The EFOS Policy Authority reviews this CP and the CPS when necessary but at least annually.

Amendments to this CP or a CPS are posted to the online repository.

9.12.2. Notification Mechanism and Period

The EFOS will notify participants upon significant changes to this CP or a CPS. Notifications shall be made through at least the following:

- Publications on EFOS website
- Newsletters
- Communication directly with accountable issuers

EFOS may, without notice, make editorial and typographical corrections and other changes that do not materially

impact the EFOS participants.

EFOS does not have a fixed notification period

9.12.3. Circumstances under which OID Must Be Changed

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

9.13. Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism the disputing party shall notify EFOS of the dispute with a view to seek dispute resolution.

Disputes that cannot be settled between EFOS and the party themselves shall ultimately be resolved within the Swedish legal system.

9.14. Governing Law

The laws of Sweden shall govern the interpretation, construction, enforcement and validity of this CP.

9.15. Compliance with Applicable Law

This CP is subject to all laws and regulations within the jurisdiction within which the EFOS PKI operates.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

See 1.1 and the EFOS membership agreement.

9.16.2. Assignment

See 1.1.

9.16.3. Severability

No stipulations.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulations.

9.16.5. Force Majeure

EFOS is not liable for a delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond EFOS reasonable control. The operation of the Internet is e.g. beyond EFOS reasonable control.

Force majeure may be regulated in the EFOS membership agreement

9.17. Other Provisions

9.17.1. Inter-Agency Agreement

Eligible Agencies or organizations wishing to participate in the EFOS PKI shall signify their acceptance of the terms of an [IAA], which shall, as a minimum, meet the requirements of [CABF] §9.3. This agreement shall be signed by each participating organizations authorized representative, per [StatsRegister]. Once signed, the Agreement shall apply to all Certificate Requests which are submitted by and signed by any Administrator, acting in an RA capacity, representing that organizations (that organizations being effectively the Subscriber).

The scope of [IAA] shall be all topics in this CPS where there is reference to [IAA] as being the applicable agreement on which operations shall be based and any other topics as deemed necessary according to the CPS, of which [IAA] shall be a subordinate document, notwithstanding its status as given by this CPS.

Acknowledgement of [IAA] shall be required by reference from each Certificate Request, thus enforcing both the Administrators (Subscribers) and individual Subjects (Sponsors) to acknowledge the existence of [IAA] and their entitlements and obligations thereunder.

Elektroniskt undertecknad av Magnus Enmarker
Datum: 2021.02.22 16:51:55 +01'00'