Swedish Public Sector Certificate Practice Statment

Key Information:

Formal title:	Swedish Public Sector Certificate Policy
OID:	1.2.752.146.200.3.1.0.0 { iso (1) member (2) sweden (752) swedish social insurance agency (146) EFOS (200.3) [cpvn-top (0) cpvn-2nd (0) cps (1)] }
Responsible authority:	EFOS Policy Authority
Version:	*1.2.5*
Effective date:	*2025-02-17*
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
1.2.5	2025-02-17	EFOS PA	Approved and Added "and/or RFC5019" in 7.3 and 7.3.2
1.2.4	2024-03-05	EFOS PA	Approved
1.2.3	2024-02-23		Changes in chapter 6.1.1, 6.2.1, 6.2.10, 9.4.1 and 9.15
1.2.2	2023-09-06		Changes in chapter 7.2
1.2.1	2023-05-24		Changes in chapter 3.1.2 and 4.1. Adding chapter 8.7
1.2.0	2021-09-22	EFOS PA	Approved
1.1.9	2021-06-08		Change in chapter 5.3.2
1.1.8	2021-05-10	EFOS PA	Approved
1.1.7	2021-05-06		Change from 18 to 19 in chapter 3.2.2
1.1.6	2021-02-22	EFOS PA	Approved
1.1.5	2021-02-08		Adding RPA in several chapters Adding OID clarification in chapter 1.2 Adding KeyUsage i chapter 1.1 and 4.5 Adding chapter 5.4.1 Adding info om system logs in chapter 5.4.4
1.1.4	2020-08-31	EFOS PA	Approved

1.1.3	2020-08-19		Change from Policy to Practice. Changes in chapter 3.2.2.4(Ballot SC27v3). Change in chapter 4 to allow Försäkringskassan to order function certificates for authority's that we operate. Changes in 6.1.2
1.1.2	2020-03-23	EFOS PA	Approved
1.1.1	2020-02-28		Changes to reflect EFOS Tillitsramverket, in chapter 4.1.2, 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.
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 1.6 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. This contract must make references to this CPS 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 CPS 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 Practice Statement (CPS) 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' 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 CPS conforms to the Internet Engineering Task Force (IETF):

- RFC3647 for Certificate Policy and Certification Practice Statement construction
- RFC2119 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 CPS 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 centers that operate in terms of a Certification Practices Statement (CPS) that complies with the requirements in this CPS.
- Relying parties who need to understand how much trust to place in an EFOS certificate, or a digital signature using an 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 CPS 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 CPS 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 CPS.

This CPS 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/signing certificates for machines/servers and shared email addresses intended to identify/sign non-human entities

1.2. Document Name and Identification

The OID for the EFOS PKI is derived thus:

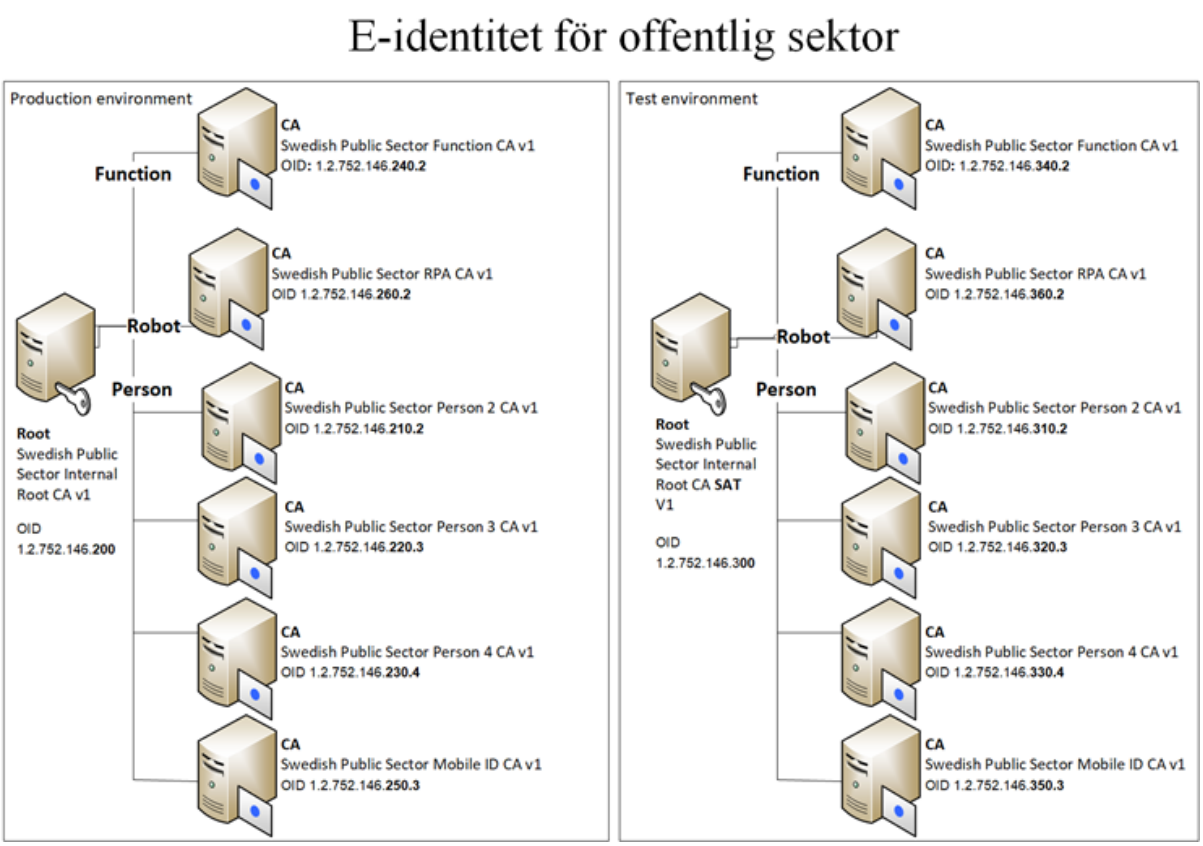
Försäkringskassan	::= { iso (1) member-body (2) sweden (752) swedish social insurance agency (146) } 1.2.752.146
EFOSRootCA	::= { EFOS 1.0 } 1.2.752.146.200

The OID for the Swedish Public Sector Person 2 CA v1 (Person 2 CA) is defined in the applicable CP as {1.2.752.146.210.2}, the OID for the Swedish Public Sector Person 3 CA v1 (Person 3 CA) is defined in the applicable CP as {1.2.752.146.220.3}, the OID for the Swedish Public Sector Person 4 CA v1 (Person 4 CA) is defined in the applicable CP as {1.2.752.146.230.4}, the OID for the Swedish Public Sector Function CA v1 (Function CA) is defined in the applicable CP as {1.2.752.146.240.2} ,the OID for the Swedish Public Sector Mobile ID CA v1 (Mobile ID CA) is defined in the applicable CP as {1.2.752.146.250.3} and the OID for the Swedish Public Sector RPA CA v1 (RPA CA) is defined in the applicable CP as {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 1.2.752.200.1.0.0.6
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 table above, in context with other CAs falling under the authority of the EFOS Policy Authority.



Picture showing OID for EFOS production and test environment.

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

1.3. PKI Participants

This CPS observes the same definitions of and roles and responsibilities for PKI Participants as described in the CP.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

See CP 1.4.1. Refer to the applicable CP.

CP	EFOS_CA_CP at https://repository.efos.se/

1.4.2. Prohibited Certificate Uses

See CP 1.4.2.

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 CPS.

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. CPS Approval Procedures

Each formal release of this CPS 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 CPS which has a **significant policy change** requiring a change of the policy’s OID

Second-level: A formal release of this CPS 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 CPS 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 CPS 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 to smart card or equal
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~~ See: Tillitsramverk för Svensk e-legitimation | Digg
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). Also called Security identity number
Relying Party	Limitations defined in §1.1but otherwise with the meaning ascribed to it in [RFC3647].
RPA	Robot, ChatBot and more are hence referred to as “RPA”.
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.~~ Statistiska centralbyrån (Statistics Sweden) [StatsRegister], available at Myndighetsregistret - SCB 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.)
- https://www.efos.se
- https://repository.efos.se
- https://aia.efos.se/

- http://crl.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

The repository is open to public access and has a stable redundant infrastructure which ensures 99% availability on a 24 / 7 basis. 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 chapter 3.3 in CP.

Email addresses can only be expressed as SMTP-addresses (IETF RFC2822 or IETF RFC5322).

See appendix 1 for details of the certificate.

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

Name uniqueness in certificates shall also be ensured by assigning each participating Agency the name given it in the register maintained by Statistiska centralbyrån (Statistics Sweden) [StatsRegister], available at ~~http://www.myndighetsregistret.scb.se/Myndighet~~ Myndighetsregistret - SCB

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**:

- Certificate application to a digital robot must be done by a dedicated physical person with at least one of the organizations within an issuance domain. For all identity 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.
- The unique identifiers are defined as automatic generated number that look like a Swedish personal identity number, but it starts with “19”. Given name will always be “RPA”.

- **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

3.2.2.1 Identity

On an initial application the Agency’s or organizations identity is recognized according to [StatsRegister].

Function CA	In the [IAA] must all addresses that the Agency want to use for Common Name (CN), be specified. All addresses are checked against https://www.iis.se/ to see if the Agency has the owner right to that address. The approved addresses are then added to the Portals whitelisted addresses for that specific Agency. When enrolling for a function certificate an automated check is made to validate the address. If other addresses (non-registered in the [IAA]) are stated in the request, that request will be rejected. Any change of addresses, must be communicated to EFOS and be added to the [IAA] or other equivalent document. EFOS confirms that the Applicant have a signed contract [IAA] and that the Agency exist, and there is a signed document with all valid Applicants. Only pre-approved domain is used.

3.2.2.2 DBA/Tradename

Function CA	EFOS don´t allow DBA or trade name.

3.2.2.3 Verification of Country

Function CA	If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using any method in Section 3.2.2.1.

3.2.2.4 Validation of Domain Authorization or Control

Function CA	EFOS may confirm ownership of domain name or IP address listed in the Certificate by using at least one of the methods listed below. EFOS will not issue Onion certificate.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Function CA	For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Function CA	EFOS may contact the Applicant with email, fax, sms or postal mail and a confirmation must then be sent back within 30 days. EFOS will initially confirms that the Applicant have a signed contract [IAA] and the Agency exist, and there are a signed document with all valid Applicants. Only pre-approved domain (checked in CAA record or [IAA] contract) registers are used.

3.2.2.4.3 Phone Contact with Domain Contact

Function CA	EFOS SHALL NOT perform validations using this method after May 31, 2019. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

3.2.2.4.4 Constructed Email to Domain Contact

Function CA	EFOS confirms that the Applicant have a signed contract [IAA] and the Agency exist (checked with www.bolagsverket.se), and there are a signed document with all valid Applicants and all contact with the Applicant only will be with the e-mail address in the signed document. EFOS will initially confirms that the Applicant have a signed contract [IAA] and the Agency exist, and there are a signed document with all valid Applicants. Only pre-approved domain (checked in [IAA] contract) registers are used.

3.2.2.4.5 Domain Authorization Document

Function CA	For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.

3.2.2.4.6 Agreed-Upon Change to Website

Function CA	Not applicable.

3.2.2.4.7 DNS Change

Function CA	Not applicable.

3.2.2.4.8 IP Address

Function CA	EFOS SHALL confirm ownership of domain name or IP address by using these methods listed in the Certificate using at least one of the methods listed above.

3.2.2.4.9 Test Certificate

Function CA	This method has been retired and MUST NOT be used. Prior validations using this method and validation data gathered according to this method SHALL NOT be used to issue certificates.

3.2.2.4.10 TLS Using a Random Number

Function CA	Not applicable.

3.2.2.4.11 Any Other Method

Function CA	This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Function CA	EFOS will confirm the Applicant’s control over the FQDN by validating the Applicant is the Domain Contact.

3.2.2.4.13 Email to DNS CAA Contact

Function CA	EFOS can confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A). Each email MAY confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated. The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values. Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.14 Email to DNS TXT Contact

Function CA	EFOS can confirm the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN. Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated. The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values. Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.15 Phone Contact with Domain Contact

Function CA	EFOS can confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. In the event that someone other than a Domain Contact is reached, the CA MAY request to be transferred to the Domain Contact. In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values. Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Function CA	EFOS can confirm the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. The CA MAY NOT knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of Domain Validation. In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values. Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.5 Authentication for an IP Address

Function CA	This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate. EFOS can confirm that prior to issuance. If we do we will validated each IP Address listed in the Certificate using at least one of the methods specified in this section. Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1 of this document) prior to Certificate issuance. For purposes of IP Address validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate. After July 31, 2019, CAs SHALL maintain a record of which IP validation method, including the relevant BR version number, was used to validate every IP Address. Note: IP Addresses verified in accordance with this section 3.2.5 may be listed in Subscriber Certificates as defined in section 7.1.4.2 or in Subordinate CA Certificates via iPAddress in permittedSubtrees within the Name Constraints extension. CAs are not required to verify IP Addresses listed in Subordinate CA Certificates via iPAddress in excludedSubtrees in the Name Constraints extension prior to inclusion in the Subordinate CA Certificate.

3.2.2.5.1 Agreed-Upon Change to Website

Function CA	EFOS can confirm the Applicant's control over the requested IP Address by confirming the presence of a Request Token or Random Value contained in the content of a file or webpage in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP Addresses, on the IP Address that is accessible by the CA via HTTP /HTTPS over an Authorized Port. The Request Token or Random Value MUST NOT appear in the request. If a Random Value is used, the CA SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1 of this document).

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

Function CA	EFOS can confirm the Applicant's control over the IP Address by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact. Each email, fax, SMS, or postal mail MAY confirm control of multiple IP Addresses. The CA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the IP Address Registration Authority as representing the IP Address Contact for every IP Address being verified using the email, fax, SMS, or postal mail. The Random Value SHALL be unique in each email, fax, SMS, or postal mail. The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

3.2.2.5.3 Reverse Address Lookup

Function CA	EFOS can confirm the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under BR Section 3.2.2.4.

3.2.2.5.4 Any Other Method

Function CA	Using any other method of confirmation, including variations of the methods defined in BR Section 3.2.2.5, provided that the CA maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described in version 1.6.2 of these Requirements. CAs SHALL NOT perform validations using this method after July 31, 2019. Completed validations using this method SHALL NOT be re-used for certificate issuance after July 31, 2019. Any certificate issued prior to August 1, 2019 containing an IP Address that was validated using any method that was permitted under the prior version of this section 3.2.2.5 MAY continue to be used without revalidation until such certificate naturally expires.

3.2.2.5.5 Phone Contact with IP Address Contact

Function CA	EFOS can confirm the Applicant's control over the IP Address by calling the IP Address Contact's phone number and obtaining a response confirming the Applicant's request for validation of the IP Address. The CA MUST place the call to a phone number identified by the IP Address Registration Authority as the IP Address Contact. Each phone call SHALL be made to a single number. In the event that someone other than an IP Address Contact is reached, the CA MAY request to be transferred to the IP Address Contact. In the event of reaching voicemail, the CA may leave the Random Value and the IP Address(es) being validated. The Random Value MUST be returned to the CA to approve the request. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

3.2.2.5.6 ACME "http-01" method for IP Addresses

Function CA	EFOS can confirm the Applicant's control over the IP Address by performing the procedure documented for an "http-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

3.2.2.5.7 ACME "tls-alpn-01" method for IP Addresses

Function CA	EFOS can confirm the Applicant's control over the IP Address by performing the procedure documented for a "tls-alpn-01" challenge in draft 04 of "ACME IP Identifier Validation Extension," available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

3.2.2.6 Wildcard Domain Validation

Function CA	The wildcard character (*, asterisk, Asterisk) is only accepted in the left label of the CN or "subjectAltName". More than one wildcard character (e.g. *.*.example.se) per CN or "subjectAltName" is not accepted. If a wildcard character appears in a label immediately to the left of a "registry-controlled" or "public suffix", the applicant MUST be rejected (e.g. "*.co.se" or "*.se"), unless the customer exercises its legal control over the entire domain name space.

3.2.2.7 Data Source Accuracy

Function CA	Not applicable.

3.2.2.8 CAA Records

Function CA	When processing CAA records, CAs MUST process the issue, issuewild, and iodef property tags as specified in RFC 6844, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. CAs MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property with this flag set. CAs MAY treat a non-empty CAA Resource Record Set that does not contain any issue property tags (and also does not contain any issuewild property tags when performing CAA processing for a Wildcard Domain Name) as permission to issue, provided that no records in the CAA Resource Record Set otherwise prohibit issuance.

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. Sequence number (ordningsnummer) is used for people who do not have a social security number or coordination number.

Individuals who have a social security number or coordination number can be assigned an additional identity if necessary, ie a Sequence number. In that case, link the Sequence number with another name to the applicant's regular person record, ie a connection to a valid social security number. Period of validity is currently at most twelve (12) months, but can be extended with further.

The figure for the century is set at 15XX for these people. Then the person's birth date is set (eg 701003).

After the punctuation mark follows four digits where the first three digits are a counter and the last digit is a check digit used to check the validity of a person number. Note that the second-last number does NOT represent the holder's gender (in the form of odd numbers for men and even numbers for women).

Example of calculating a Sequence number:

For the first person for a specific date, a counter is set to 001, the subsequent to 002, and so on.

The Sequence number of the first man or woman born on October 3, 1970 will be: 15701003–0018. The next person born on the same day will receive the following Sequence number: 15701003–0026

If Sequence number runs out during 15XX, 14XX will be used.

All Sequence number uses identity assurance level 2.

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” or “Swedish Government Auth CA v2” with 2 years validity to individuals with identity assurance level 3.

3.2.6. Criteria for inter-operation

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

Re-keying is not allowed

3.3.2. Identification and authentication for re-key after revocation

Re-keying is not allowed

3.4. Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, either the certificate subscriber, id-administrator or authorized applicant within the issuance domain or EFOS Operational Authority verifies that the revocation has been legitimately requested if the requester has been logged in to the Portal and asked for revocation. The revocation is then effected and published automatically.

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

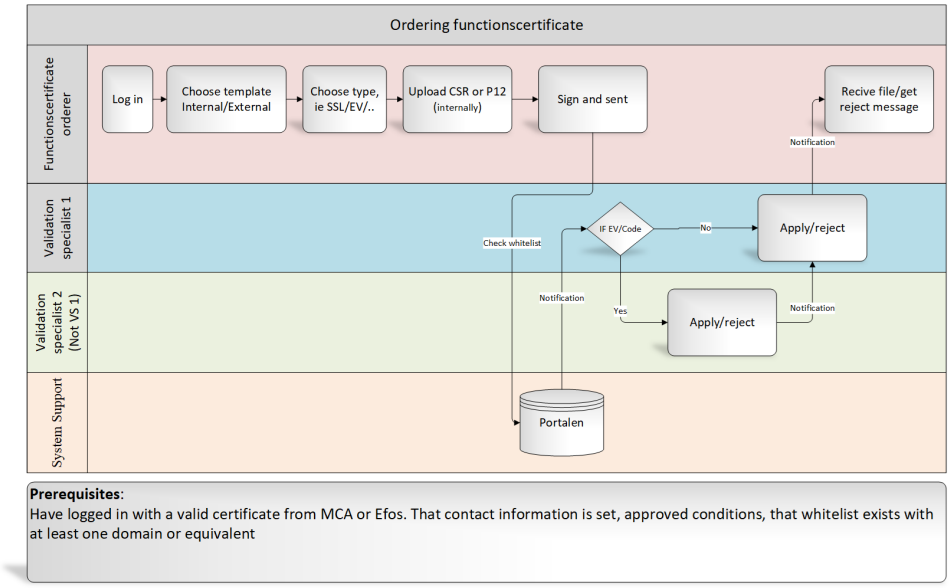
Försäkringskassan has the possibility to submit a certificate application on behalf of an agency, if we operate the authority's web services and these require a certificate. However, this must be stated in the agreement [IAA] before actions can be taken.

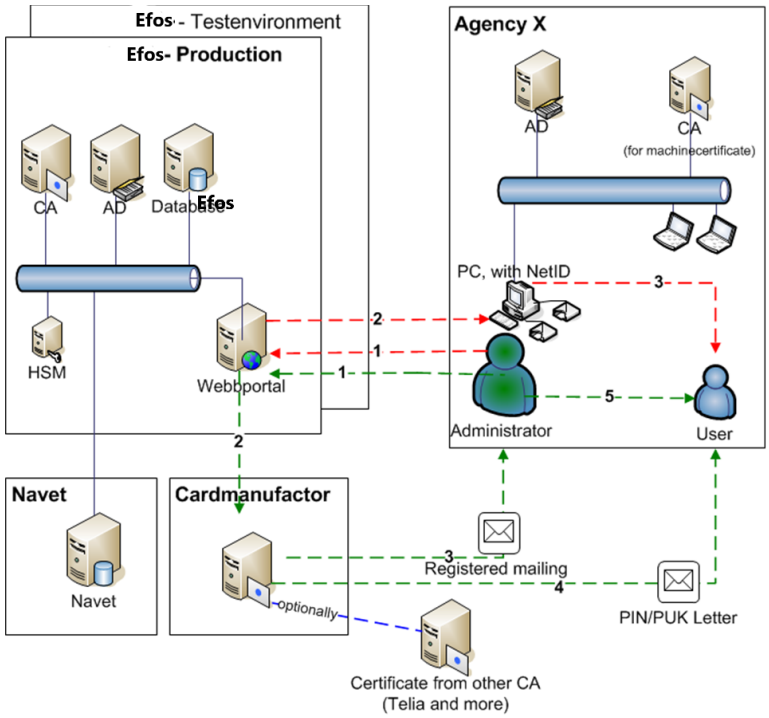
4.1.2. Enrollment Process and Responsibilities

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.

Function CA	Requesters must send request in mail with CSR or complete the online forms at website, otherwise EFOS can´t approve the certificate Application.  The process of requesting a certificate is illustrated above. The organization Registration Agent requester needs to be in the correct role, accept terms and have a valid certificate from “Person 3 CA”, “Person 4 CA” or “Swedish Government Auth CA v2” with 2 years validity to be able to make a certificate request. From the Portal the RA have the possibility to see requests from its organization and have the possibility to revoke a certificate if the private key is lost or compromise or if there is other valid reasons. Validation specialist needs to accept all domains/ip for requesting organisations before they can request certificate. When they apply Validation specialist needs to apply/deny all certificate request. Försäkringskassan has the opportunity to enrol for a server certificate on behalf of an agency, if we operate the authority's web services and these require a certificate. However, this must be stated in the agreement [IAA] before actions can be taken.
RPA CA	Authorized applicants within the issuance domain have the utmost responsibility in validating the application itself as well as the identity of the RPA/robot. All validations shall be done in accordance with the issuance routines, prior to authorizing issuance of a certificate. Each Applicant shall submit sufficient information and documentation for the RPA/robot 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.
MobileID CA	The process of requesting a certificate is for an end user with a valid certificate from “Person 3 CA”, “Person 4 CA” or “Swedish Government Auth CA v2” with 2 years validity to be able to make a certificate request. The user needs to accept terms before they can download a MobileID certificate after present an activation code to a smart phone or equal from a self-service portal. There they can request and revoke personal certificate.
Person 2-4 CA	



Flow for issuing an ordinary smart card (LoA 4 or 3):

1. Central administrator logs on to the Web portal and order cards
2. Certificate is sent to the card provider of card (e.g. e-leg)
3. Card provider sends cards to administrator with REK
4. PIN/PUK code is sent by mail to the Applicant
5. Local administrator is handing out cards to Applicant by id control

Flow for Temporary cards/spare cards (LoA 3 or 2):

1. The Applicant's id checked and the Local administrator logs on to the Web portal. The Applicant's personal identification number or coordination number is entered. If the Applicant has a short contract and don´t have a social security number or coordination number, the sequential number (ordningsnummer) could be generated (for the Applicant) by the administrator in a separate routine. Level of Assurance (LoA) is determined by the Applicants possibility to prove identity and the possibility to dial to the Applicant, have another person to validate the Applicant identity or other method.
2. Certificates are created and are written down to the card
3. The Applicant receives cards and can start working immediately

There is a possibility to remote publishing of cards (LoA 2):

1. The Foreign Manager (FM) contacts the Swedish Manager (SM) when a user needs an eID.
2. The FM takes a photo of the Applicants passport and sends it to the SM.
3. The FM contacts the SM who fills a form with the Applicants information and ends it with a digital signature. Temporty card is sent to the Applicant.
4. The SM brings the form to a Local administrator who in the portal registers the card number of a temporary card for the sequential number and the ID of the SM in the role as certifier.
5. The administrator calls the Applicant.
6. The Applicant logs on to the selfservice portal with a temporary code, puts the temporary card in a card reader and accept terms, certificates are created and written to the card.
7. The Applicant can start working immediately

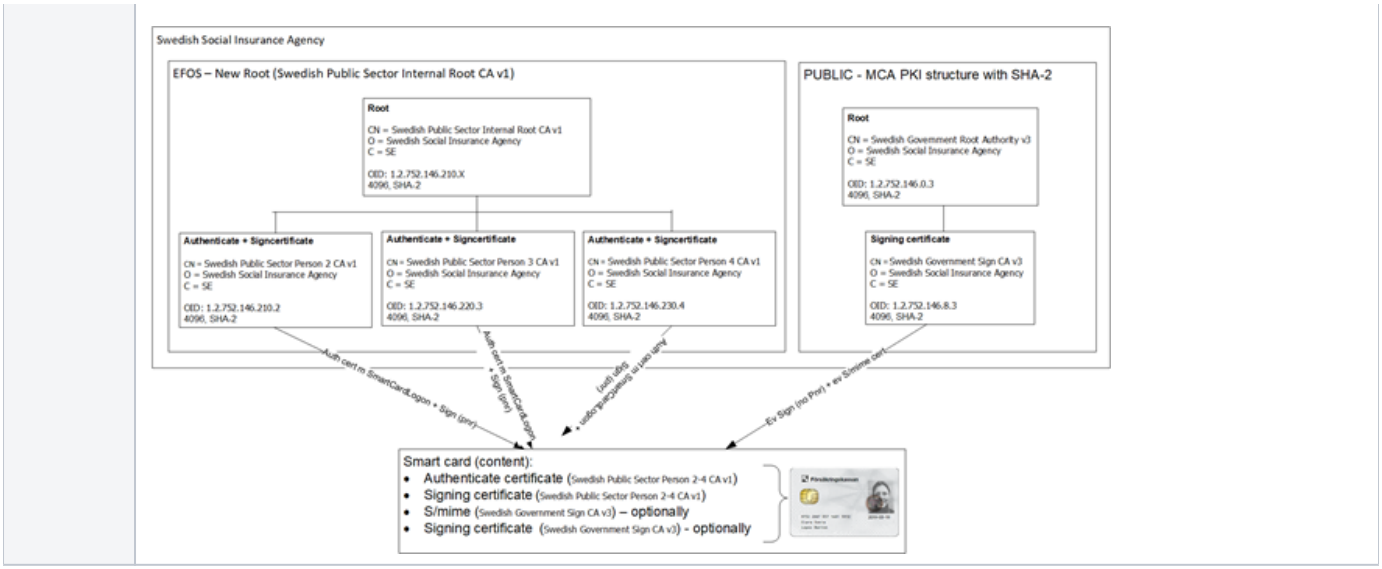
Applicant with coordination number or the sequential number can only apply for LoA2 certificates.

Requesters must complete the online forms at website, otherwise EFOS can´t approve the certificate Application.

The process of requesting a certificate is illustrated above. The Agency Registration Agent requester needs to be in the correct role and have a valid certificate from “Person 3 CA”, “Person 4 CA” or “Swedish Government Auth CA v2” (with more than 2 years validity) to be able to make a Sign CA certificate request.

From the Portal the Administrator have the possibility to see requests from its organization and have the possibility to revoke a certificate if the private key is lost or compromise or if there are other valid reasons.

On the Applicant´s smart card there will be (at least) two certificates, one Authenticate and one signing certificate from “Person 2 CA”, “Person 3 CA”, “Person 4 CA” see below. There is an option to add other certificates from “Sign CA”.



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 the 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 any of 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 verify that the information regarding the individual is up to date with the Tax Agency (NAVET) where 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 individuals:

- When signing a receipt for an EFOS E-id for individuals with a certificate on 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 will 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 and functions they need to accept terms and conditions when requesting.

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 a robot/RPA
- Function – TLS/signing certificates for machines/servers and shared email addresses intended to identify/sign 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 see https://repository.efos.se.

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 CPS. 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
    - 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. Notification of new certificate issuance to subscriber

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. Notification of certificate issuance by the CA to other entities

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 CPS. 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 CA v1 to CA v2) 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 Certificate Modification to Subscriber

See 4.8, 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 Modification 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 CPS
- 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 centres.
- 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.

If an organization terminates its relationship with the EFOS, then shall EFOS revoke all certificates issued in the name of that organization.

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

When required by law or other explicit policy or directive, EFOS or the RA may notify law enforcement. Revocation leads to several updates in the database; the immediate update of OCSP service and next update of CRL. A revoked certificate shall continue to be in CRL until the certificate expires.

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 CPS 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

CRLs are posted to the repository within four hours of generation (and no later than 18 hours after notification of compromise) after generation.

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. Upon system failure or other factors that are not under the control of the CA, EFOS shall make best endeavour's to ensure that this information services are not unavailable for an unreasonable long period of time.

4.10.3. Operational 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 performs 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 employ active surveillance and alarms that are monitored by guards 24 hours every day of the year.

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 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 are either 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 have:

- 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 have a back-up power supply and sufficient environmental controls to protect the CA systems. There are primary and secondary power supplies that ensure continuous, uninterrupted access to electric power. Redundant backup power is provided by battery uninterrupted power supplies (UPS) and diesel generators.

The facility is equipped with heating, ventilation, and air conditioning appropriate for a commercial data processing facility.

5.1.4. Water Exposure

EFOS has taken reasonable precautions to minimize the impact of water exposure to the CA system. No liquid, gas, exhaust, etc. pipes traverse the controlled space other than those directly required for the area’s HVAC system and for the pre-action fire suppression system.

5.1.5. Fire Prevention and Protection

The secure facility is equipped with fire suppression.

5.1.6. Media Storage

All media containing production software and data, audit, archive, or backup Information is stored within EFOS facilities and in a secure off-site storage facility with appropriate physical and logical access controls.

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 performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner. Access to the site is limited to authorized personnel listed on an access list, which is subject to audit. Since the document classification of the CPS is “un-classified” further details cannot be shared in the CPS. There is a separate internal EFOS document that provides more details.

5.2. Procedural Controls

5.2.1. Trusted Roles

Personnel acting in Trusted Roles include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

the validation of information in Certificate Applications;

the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrolment information;

- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

CA Trusted Roles include, but are not limited to:

- PKI Administrator
- System Administrator/ System Engineer (Operator)
- Agency Registration Agent/ Server Administrator

- Internal Auditor Role
- External Auditor Role

Persons seeking to acting in Trusted Roles must successfully complete the screening requirements set out in this CPS. All personnel in Trusted Roles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations. Senior management of the EFOS shall be responsible for appointing individuals to Trusted Roles).

There is a separate document that specifies Trusted Roles in detail. Since the document classification of the CPS is “un-classified” further details cannot be shared in the CPS. There is a separate internal EFOS document that provides more details.

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 CPS.

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 id-administrator within an issuance domain and the person utmost responsible for issuance of certificates. Has the system role “Ansvarig utgivare” or equal.

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 centres
- Access to subscriber activation data during generation at Processing centres

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

Each person fulfilling a Trusted Role must undergo checks and identification prior to acting in the role, including verification of the individual's identity, employment history, education, character references, social security number and other relevant background information. This procedure may be performed by the recruiting chief, the human resources department or other suitable department. The background investigations may be performed by SÄPO (Swedish Security Service) which is a competent independent authority that has the authority to perform background investigations. Agencies that are unable or can´t use this method by law, need to, use the predefined process by EFOS PA or establish their own process which need to be accepted by EFOS PA before using it. The EFOS PKI shall require each individual to appear in-person before a Trusted Agent whose responsibility it is to verify identity. The Trusted Agent must verify the identity of the individual using at least one form of government-issued photo identification. If SÄPO is used, the checks are for the prior five years and will continue until the service is terminated.

These checks need not be repeated if the person concerned is already employed by the Swedish government and has been previously been subjected to these checks, but in the case that they have not been subjected to these checks they shall be performed within a period of three (3) months of the publication of this CPS and thereafter prior to appointment for new personnel.

5.3.3. Training Requirements

EFOS provides all personnel with training skills that covers basic Public Key Infrastructure (PKI) knowledge, authentication and verification policies and procedures, common threats to the validation process, including phishing and other social engineering tactics, and the Guidelines. Training of personnel is undertaken via a mentoring process involving senior members of the team to which they are attached. All new personnel must undergo this training process for at least two months. EFOS maintain records of such training and ensures that personnel entrusted with Trusted Roles meet a minimum skills requirement that enable them to perform such duties satisfactorily. EFOS ensures that its personnel qualify for each skill level required by the corresponding task before granting privilege to perform said task.

All training materials will 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

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in Trusted Roles. EFOS PKI make individuals acting in Trusted Roles aware of any changes to the EFOS PKI and RAs' operations. If such operations change, the EFOS PKI shall provide documented training, in accordance with an executed training plan, to all Trusted Roles. EFOS provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

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

In limited circumstances, independent contractors or consultants may be used to fill trusted positions. They are held to the same functional and security criteria that apply to an EFOS employee in a comparable position.

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 log files are generated for all events relating to the security and services of the EFOS components. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and nonelectronic, shall be retained and made available during compliance audits. EFOS ensures all events relating to the life cycle of certificates are logged in a manner to ensure the imputability to a person in a trusted role of an action required for EFOS services.

5.4.1. Types of Events Recorded

EFOS manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by EFOS personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry
- Identity of the entity making the entry
- Kind of entry.

EFOS log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant
- Record of unique identification data, numbers, or a combination thereof (e.g., driver’s license number or equal) of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA, if applicable.

5.4.2. Frequency of Processing Log

EFOS PKI review logs at least every two months, review the audit log to trace and investigate events that occurred. The review includes verification of the audit log for alteration; viewing all items in the log and checking for warnings or anomalies; and explanation of the causes of such events and proposition of preventive actions. Actions taken based on log reviews are also documented. Log files and audit trails are archived for inspection by the authorized personnel of EFOS and designated auditors.

5.4.3. Retention Period for Audit Log

Records concerning EFOS PKI logs are held for a period of time (10 years) as appropriate for providing necessary legal evidence in accordance with the applicable legislation. EFOS system logs are held for a period of 3 years.

5.4.4. Protection of Audit Log

Audit logs are protected by physical and electronic security measures, and kept open for access by authorized personnel only.

5.4.5. Audit Log Backup Procedures

Audit logs and audit summaries are backed-up in a secure location, under the control of an authorized trusted role, separated from their component source generation. Audit log backup is protected to the same degree as originals.

5.4.6. Audit Collection System (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by authorized personnel only.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

Vulnerability scans and penetrations tests will be performed in accordance with guidelines from CA Browser Forum. Any findings are documented and prioritized on severity by those performing the test.

EFOS and accountable issuers will 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 will 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 PKI includes sufficient detail in archived records to show that a certificate was issued in accordance with the CPS.

EFOS retains in a trustworthy manner records of EFOS digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

CA and RA archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data shall be archived:

- All logs in §5.4.1 (CP);
- EFOS CA audit documentation;
- EFOS CA CP documents (all versions);
- EFOS CA CPS documents (all versions);

5.5.2. Retention Period for Archive

EFOS CA retain archived data for at least ten (10) years unless a greater retention is required by any other applicable law, standard, policy, etc. System logs are held for a period of 3 years.

5.5.3. Protection of Archive

Archive records are stored at a secure off-site location and are protected by physical and electronic security measures, and kept open for access by authorized personnel only. Electronic archives are protected against unauthorized viewing, modification or deletion. Archives on paper are retained in special units to which only authorized personnel can access.

5.5.4. Archive Backup Procedures

According to the EFOS backup and disaster recovery operating procedures, key, certificate and transaction data should be archived and backed up daily, weekly and monthly. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5. Requirements for Time-stamping of Records

All records in the database and in log files are time-stamped using the system time of the system where the event is recorded. The system time of all servers is synchronized with the time source of RISE (http://www.ntp.se/) using the Network Time Protocol (NTP).

5.5.6. Archive Collection System (internal or external)

EFOS will collect archive information internally.

5.5.7. Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored

5.6. Key Changeover

EFOS CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS. EFOS CA certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs can be generated for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services.

Key changeover procedures enable the transition from expiring CA certificates to new CA certificates. Towards the end of the CA private key's lifetime, EFOS CA ceases using its expiring CA private key to sign certificates no later than 60 days before the point in time where the remaining lifetime of the expiring CA key pair equals the approved certificate validity period for the specific type(s) of certificates issued. The old private key is only used to sign CRLs until the expiration date of the last certificate issued using the original key pair has been reached.

A new CA signing key pair is commissioned and all subsequently issued certificates and CRL's are signed with the new private signing key. Both the old and the new key pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP. EFOS maintains backups of the foregoing CA information for their own CAs.

EFOS establishes business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or compromise the EFOS PKI services. EFOS PKI carries out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary (threat evolution, vulnerability evolution etc.). This business continuity is in the scope of the audit process as described in section 8 to validate what are the operations that are first maintained after a disaster and the recovery plan. EFOS personnel that own a trusted role and operational role are specially trained to operate according to procedures defined in the Disaster Recovery plan for the most sensitive activities. If EFOS detects a potential hacking attempt or another form of compromise, it should perform an investigation in order to determine the nature and the degree of damage. Otherwise, the EFOS PKI assesses the scope of potential damage in order to determine whether the CA or RA system needs to be rebuilt, whether only some certificates need to be revoked, and/or whether a CA hierarchy needs to be declared as compromised. The EFOS disaster recovery plan highlights which services should be maintained (for example revocation and certificate status information).

There is a separate document that specifies this in detailed. Since the document classification of the CPS is "un-classified" further details cannot be shared in the CPS. There is a separate internal EFOS document that provides more details.

The EFOS PKI has implemented a data back-up and recovery procedures and have developed a Disaster Recovery (DR) and/or Business Continuity Plan (BCP). The EFOS PKI shall have redundant CA systems that are located at a separate, geographically diverse location and that are configured for automatic failover in the event of a disaster (Disaster Recovery/Mirror Site). The EFOS PKI shall review, test, and update the DR/BCP and supporting procedures annually. If a disaster occurs, the EFOS PKI shall re-establish operational capabilities as quickly as possible.

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

EFOS PKI performs system back-ups on a daily basis. Back-up copies are made of EFOS CA:s Private Keys and are stored off-site in a secure location. In the event of a disaster whereby the primary and disaster recovery CA operations become inoperative at EFOS primary facility and the Disaster Recovery / Mirror Site, EFOS PKI will re-initiate its operations on replacement hardware (on-site) using backup copies of its software, data and CA private keys at a secured facility.

If it cannot be made fully operational or some of the records cannot be recreated, all subscribers and relying people that may be affected shall be urgently notified. Where necessary, certain certificates shall be revoked and new certificates shall be issued.

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.

Prior to termination by deletion EFOS shall publish a notification to this effect to EFOS online repository no less than one (1) year (365 days) in advance.

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
- Revoke all certificates that are still un-revoked or un-expired at the end of one (1) year (365 days) notice period without seeking Subscriber's consent.
- Ensure that all archived information and logs are kept for the entire duration of the archival period

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

EFOS will 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.

Function CA	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
MobileID CA	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 NIST SP800-90A
RPA	Subscriber private keys are be generated using a FIPS-approved method. Generation subscriber private keys for RPA are: • 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 EAL6+ and use a random number generation according to NIST SP800-90A. • If the method for issuing is PKCS#12 – Generated by the EFOS-portal
Person 2-4 CA	Subscriber private keys are be generated using a FIPS-approved method. • Generation subscriber private keys for persons are: • 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 EAL6+ and use a random number generation according to NIST SP800-90A.

EFOS 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 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.

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.

Function CA	Subscribers are solely responsible for the generation of the private keys used in their certificate requests (CSR). If there isn't a CSR the EFOS PKI creates the certificate from user input and generates a password for that certificate with a random module. That password is not kept in the system after the certificate is generated. The end-user must collect it and store it safely.

	For certificate from “Swedish Government HW CA v4” the user must provide CSR.
MobileID CA	An identification of the subscriber will always be preceded before a Subscriber could get certificate. Activation code is delivery to a Subscriber during registration process. End-user subscriber key pairs are generated on smart phone. Subscribers shall sign a receipt in connection to delivery of a private key.
RPA	End-user subscriber key pairs are generated by EFOS Portal
Person 2-4 CA	End-user subscriber key pairs are generated by a processing center. PIN/PUK is delivery to a Subscriber through mail. Smart card is delivered to Local admin. An identification of the subscriber will always be preceded before a Subscriber could get smart card (or equal) with certificate. 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 in the responsibility of the entity holding it.

6.1.3. Public Key Delivery to Certificate Issuer

Function CA	Public key will be able to receive from Portal or through e-mail.
MobileID CA	End-user subscriber public key are generated on end-user device.
Person 2-4 CA	End-user subscriber public key are delivered with the private key.

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:

1. The PKI repository
2. 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:

1. 2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256);
2. 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. EFOS uses RSA with 4096 for Root and Issuing CAs.

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 (see https://repository.efos.se for details).

6.2. Private Key Protection and Cryptographic Module Engineering Control

The procedures dictated by this CPS 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.

EFOS use HSM, certified to FIPS 140-2 level 3, to protect the Certification Authorities' Private Keys.

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 EAL6+.
- 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 does 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 are 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 store its CA Private Keys on a cryptographic module which has been evaluated to at least FIPS 140-2 Level 3.

Subscriber private keys will be stored according to 6.2.1

6.2.8. Method of Activating Private Key

EFOS 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 are 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 (decision for destruction will be made in a "IT-tjänsteforum") 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 shredded the smart card by an 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, 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 RPA Certificate	3 years	3 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 will 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) will be generated with good entropy and using multi-person control according 5.2.2
- Chosen by the subscriber as part of the certificate (mobile ID) issuance process. Subscribers shall choose activation data with good entropy.

6.4.2. Activation Data Protection

EFOS CA 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 require EFOS PKI personnel to memorize and not write down their password or share their passwords with other individuals. EFOS may 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.

6.4.3. Other Aspects of Activation Data

Activation data for CA private keys shall be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in Section 5.5.2 lapse, EFOS shall decommission activation data by overwriting and/or physical destruction.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

EFOS will 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 may 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 server involved with PKI operations.

6.6.2. Security Management Controls

EFOS has mechanisms in place to control and monitor the security-related configurations of its CA systems. Change control processes consist of change control data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, EFOS can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. Network Security Controls

EFOS CA system is connected to one internal network and is protected by firewalls, a Demilitarized Zone (DMZ) and Network Address Translation for all internal IP addresses. EFOS customer support and vetting workstations are also protected by firewalls and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems. EFOS block all ports and protocols and open only necessary ports to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. All firewall configurations and changes thereto are documented, authorized, tested and implemented in accordance with change management policies and procedures. EFOS network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8. Time-stamping

System time for EFOS computers is updated from The Swedish national time scale, UTC (by RISE) is a national realisation of the Coordinated Universal Time, using the Network Time Protocol (NTP) to synchronize time.

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 RFC5280.
- 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) memberbody(2) us(840) rsadsi (113549) pkcs(1) pkcs1(1) 5}
SHA256WithRSAEncryption	{iso(1) memberbody(2) us(840) rsadsi (113549) pkcs(1) pkcs1(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

For revoked issuing CAs, the CRLReason indicated cannot be unspecified (0) or certificateHold(6). If the reason for revocation is unspecified, EFOS will omit the reasonCode entry extension, when technically not capable of issuance. If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate unless the reason is unspecified. EFOS specifies the following reason codes from RFC 5280, section 5.3.1 as appropriate for most instances when used in accordance with the practices in this section and this CPS:

- **keyCompromise (RFC 5280 CRLReason #1)**
- **affiliationChanged (RFC 5280 CRLReason #3)**
- **superseded (RFC 5280 CRLReason #4)**
- **cessationOfOperation (RFC 5280 CRLReason #5)**
- **privilegeWithdrawn (RFC 5280 CRLReason #9)**

7.2.1. Version number(s)

EFOS issues version two (2) CRLs. CRLs conform to RFC 5280 and contain the basic fields listed below:

- Version
- Issuer Signature Algorithm
- Issuer Distinguished Name
- thisUpdate
- nextUpdate
- Revoked certificates list
    - Serial Number
    - Revocation Date

7.2.2. Issuer's SignatureCRL and CRL Entry Extensions

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

7.3. OCSP PROFILE

The EFOS PKI operate an OCSP service in accordance with RFC6960 and/or RFC5019.

7.3.1. Version Number(s)

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

7.3.2. OCSP Extensions

The EFOS PKI OCSP extensions conform to the Extensions profile in RFC6960 and/or RFC5019.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or Circumstances of Assessment

An annual audit is performed by an independent external auditor to assess EFOS compliance with this CPS.

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 http://www.webrust.org
- 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 auditors shall cover EFOS adherence to at least the following:

That EFOS and all issuance domains comply with the requirements of this CPS and the EFOS trust framework.

That this CPS 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 CPS 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 http://www.webtrust.org
- CA Browser Forum Baseline Requirements, published at http://www.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 CPS. 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.

8.7. SELF-AUDITS

Audits will be at the discretion of EFOS to gain reasonable assurance of compliance to applicable program requirements according to Audit plan for the service.

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 CPS 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 centres 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 CPS 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 processes personal data in accordance with the agreement with the customers and the European general data protection regulation (EU) 2016/679, hence referred to as “Dataskyddsförordningen”. 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 CPS. 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 CPS, the applicable CPS and all other stipulations referenced in these documents.

9.6.2. RA Representations and Warranties

Accountable issuers warrant that they comply with the requirements of this CPS, 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 CPS 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 CPS 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 CPS and any amendments are effective according to the effective dates set forth in conjuction with the publication of the CPS to the EFOS repositories, see 2.1. Each CPS 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 (730 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 CPS, 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 CPS or the CP. Controls are in place to ensure that this CPS and the CP is not amended and published without the prior authorization of the EFOS Policy Authority. The EFOS Policy Authority reviews this CPS and the CP when necessary but at least annually.

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

9.12.2. Notification Mechanism and Period

The EFOS will notify participants upon significant changes to this CPS or a CP. 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 CPS 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 CPS.

9.15. Compliance with Applicable Law

This CPS is subject to all laws (Regulation of the European Parliament and of the Council (Europaparlamentets och rådets förordning (EU) 2016/679) and Public Access to Information Act (Offentlighets- och sekretesslag 2009:400) and Act (2018:218) with supplementary provisions to the EU's data protection regulation (Lag 2018:218 med kompletterande bestämmelser till EU:s dataskyddsförordning) and other 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 CPS 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

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.

Appendix 1

See https://repository.efos.se for certificate content and profile.

See https://repository.efos.se/EFOS_Person_EndEntityCertificates.pdf for personal certificate.

See https://repository.efos.se/EFOS_MobileID_EndEntityCertificates.pdf for personal mobile certificate.

See https://repository.efos.se/EFOS_Function_EndEntityCertificates.pdf for functional certificate.

See https://repository.efos.se/EFOS_RPA_EndEntityCertificates.pdf for RPA certificate.