Author		Dodument		
Joakim Stenius		Swedish National Certificate Policy		
		Datum	Rev	D.nr
		2018-08-14	2.0	

Swedish National Certificate Policy

for the Extended Access Control Infrastructure for passports and travel documents issued by EU member states

TABLE OF CONTENT

1 INTRODUCTION 3

1.1 Terminology, Definitions and Acronyms 3
1.2 Overview 3
1.3 Document name and identification 3
1.4 PKI Participants 3
1.5 Policy Administration 7

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 8

2.1 Repositories 8

3 IDENTIFICATION AND AUTHENTICATION 9

3.1 Naming 9
3.2 SE Naming Convention 9
3.3 Registration 10

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 12

4.1 Certificate Profile 12
4.3 Successive Certificates and Requests (Re-key) 12
4.4 Certificate Appliacation and Issuing 13
4.5 Certificate Acceptance 18
4.6 Certificate Usage 18
4.7 Certificate Validity Periods 19

5 SECURITY REQUIREMENTS 20

5.1 Physical Controls 20
5.2 Procedural Controls and System Access Management 20
5.3 Incident handling 24
5.4 CVCA or DV Termination 25

6 KEY PAIR SECURITY 27

6.1 Key Pair Generation 27
6.2 Private Key Protection and Cryptographic Module Engineering Controls 27

7 COMPLIANCE AUDIT AND OTHER ASSESSMENT 29

Appendix A - Definitions and Acronyms 30
Appendix B Hardware Requirements 33

1 INTRODUCTION

This is the Swedish National Certification Policy. Requirements from the Common Certificate Policy are included into this policy.

The goal of the Certificate Policy (CP) is to achieve trust and sufficient interoperability between the Country Verifying Certification Authorities (CVCAs) and Document Verifiers (DVs) of different Member States for the EAC-PKI to operate.

The Certificate Policy only concerns the use of certificates to control access to biometrics on Extended Access Control enabled machine readable documents.

This Certificate Policy is based on the Technical Guideline:

- Common Certificate Policy for the Extended Access Controll Infrastructure for Passports and Travel Documents Issued By EU Member States, Version 2.1, BSI TR-03139, further referred to as TR-EAC
- Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Version 2.21, TR-03110, published by the Bundesamt fur Sicherheit in der Informationstechnik, further referred to as BSI-EAC
- Country Verifying Certification Authority Key Management Protocol for SPOC, CSN 36 9791 Version 1.0 published by CESCA TECHNICKA NORMA, further refered to as CSN-SPOC

1.1 Terminology, Definitions and Acronyms

As described in section 1.1: BSI TR-03139 version 2.1 of May 27th 2013.

1.2 Overview

As described in section 1.2: BSI TR-03139 version 2.1 of May 27th 2013.

1.3 Document name and identification

The following OID are used for identification of the Swedish National Certificate Policy:
1.2.752.84.101.1.1

1.4 PKI Participants

This section gives an overview of the Certification Authorities, Certificate Holders, Registration Authorities, and Relying Parties of the Extended Access Control Public Key Infrastructure (EAC-

PKI). The EAC-PKI is part of the international security infrastructure to ensure and verify integrity and authenticity of MRTDs issued by a Member State.

	Certification Authority	Registration Authority	Subscriber	Relying Party
National PKI Co-ordinator		X		
SPOC		X		X
CountryVerifying Certification Authority (CVCA)	X	X		X
Document Verifier (DV)	X	X	X	X
Inspection System (IS)			X	X
Machine Readable Travel Document (MRTD)				X

Table 1 Overview of PKI participants of the Swedish EAC-PKI

1.4.1 National PKI Co-ordinator

Sweden has one[1] named National PKI Co-ordinator who is fully responsible for interacting with foreign Member States with respect to exchange of DV-certificates and the Swedish National Certificate Policy. The PKI Co-ordinator is the only contact point and is responsible for distribution of ePassport and eResidence Permit EAC-PKI certificate issues towards foreign Member States for every action or incident of the domestic CVCA, DV and IS.

The Swedish PKI Co-ordinator ensures that the information received from Member States will be distributed to its domestic SPOC, CVCA and DV as needed for the security and functionality of their duties.
The Swedish National PKI Co-ordinator ensures that information concerning incidents such as key compromise or misuse, and suspension of CVCA, DV and IS are shared with Member States.

1.4.2 Certification Authorities

Country Verifying Certification Authority
The Root Certification Authority (CA) of the Swedish national EAC-PKI is called a Country Verifying Certification Authority (CVCA). The public keys of the Swedish CVCA are contained in both self-signed CVCA certificates and link CVCA certificates. Both classes are called CVCA certificates. The Swedish CVCA determines the access rights to sensitive data stored on domestic MRTD chips for all DVs (i.e. the Swedish DV as well as foreign DVs) by issuing DV certificates entitling access control attributes.

[1] which should usually be a defined group of persons as a subsection of a governmental office for substitution purposes

The Swedish CVCA issues certificates to its Certificate Holders (Subscribers). In this document, a Certificate Holder is called a Document Verifier (DV). A DV is an organisational unit that manages inspections systems belonging together.

For the purposes of the remainder of this document the Registration Authority (RA) will be assumed to be part of the CVCA and only the term CVCA will be used.

Document Verifier Certification Authority
Sweden has only one certification authority at the level of a Document Verifier (DV).

The Swedish DV operates a CA (DVCA) to issue certificates for its inspection systems. The inspection system certificates issued by the Swedish DV, inherits both the access rights and the validity period from the underlying DV certificate. However, the Swedish DV may choose to further restrict the access rights or the validity period of IS certificates.

1.4.3 Registration Authorities

In order to facilitate the issuance of certificates and to increase security, most of the duties of the Swedish RA are shifted to the Swedish CVCA. Communication with foreign Member States and initial registration of foreign Member States CVCAs is done by the National PKI Co-ordinator

Country Verifying Registration Authority
The Swedish CVCA has only one Registration Authority, i.e the national Country Verifying Registration Authority (CVRA). In Sweden the CVRA is operated by the same authority as the CVCA.

The Swedish CVCA is responsible for:

- the registration of the Swedish DV and the registration of foreign Member States CVCAs which shall be authorised to read sensitive data from Swedish MRTDs;
- providing and changing needed suspension status of registered DVs and CVCAs, both domestic and foreign.
- the listing of foreign DVs including their suspension[2] status;
- performing identification and authentication of certificate requests of Document Verifiers;
- suspension of the Swedish DV if they are no longer allowed to request certificates especially from foreign Member States;
- the suspension of the registration of foreign Member States in case of security incidents;
- giving information to all foreign Member States if the domestic DV is not longer allowed to request certificates from those Member States and thus is suspended;
- initiating the issuance of certificates to Document Verifiers;

Document Verifier Registration Authority
Sweden operates only one Registration Authority for its Document Verifier. i.e the national Document Verifying Registration Authority (DVRA). In Sweden the DVRA is operated by the same authority as the DV.

[2] refer to chapter 1.1 Definitions for the definition of suspension

The Swedish DV is responsible for:

registration of Swedish Inspection Systems;
performing identification and authentication of certification requests of Inspection Systems;
suspension of Swedish Inspection Systems if they are not longer allowed to request certificates;
forwarding information about security incidents of the DV itself or its maintained Inspection Systems immediately to the Swedish CVCA;
initiating the issuance of certificates to Inspection Systems;

1.4.4 Subscribers

Subscribers under this policy are Document Verifiers (DV) and Inspection Systems (IS). A DV is defined in Section 1.4.2.

For the purposes of this Certificate Policy an Inspection System (IS) is defined as the infrastructure, hardware and software required to obtain certificates from a DV, store and manage those certificates, and to obtain biometrics from MRTDs using those certificates, including mechanisms controlling access to the inspection systems.

1.4.5 Relying Parties

Relying Parties within an EAC-PKI are Document Verifiers, Inspection Systems, and MRTDs.

A relying party is an entity who verifies the signature of a certificate using a trusted certification path (see section 4.6). Sweden identifies which trusted certification path a relying party has to use in order to verify a Swedish certificate (see section 1.4).

1.4.6 SPOC Communication between participants

The Swedish SPOC (Single point of contact) acts as an interface for communication between Member States. It allows for efficient communication to carry out regular key management related tasks. Technical details of SPOC are defined in CSN-SPOC.

Sweden operates one SPOC which is compliant with the additional requirements specified in CSN-SPOC. That means that the Swedish SPOC is the technical communication interface towards other Member States concerning ePassport and eResidence Permit EAC-PKI certificate issues.

All communication with other Member States concering the Swedish CVCA and DV is carried out using the Swedish SPOC. All key management related tasks are also carried out by using Swedish SPOC.

As an additional communication channel, email is used especially to cover situation when the Swedish SPOC communication channel is not available. The email address used in this context is part of the Swedish SPOC registration form. This means that states can use email communication for manually exchanging request/certificates even if the automatic SPOC system of one or both states hasn't been implemented yet or when it is out of order.

In the event of a planned disruption of the Swedish SPOC, Sweden will notify all registered Member State's SPOC that Certificate Requests are to be submitted by email. The email address used in this context is part of the Swedish SPOC registration form. This is done in a time-frame which minimises the risk of current certificates expiring. When normal SPOC communication is resumed, Sweden will inform all registered Member State's SPOCs via General Message according to CSN-SPOC.

Both, SPOC and email communication SHALL only be used after a successful diplomatic exchange of the registration information.

1.5 Policy Administration

1.5.1 Organization administrering the document

The organization administrering this policy is the Swedish Police Authority (Polismyndigheten).

1.5.2 Contact person

All questions about this policy should be directed to:

Swedish Police Authority
Information Technology Department, eMRTD
P.O.Box 12256
SE - 102 26 Stockholm
Phone: +46 77 114 14 00
e-mail: emrtd-spoc@polisen.se

2 Publication and Repository Responsibilities

Sweden provides contact details for its national CVCA and DV to the European Commission who is responsible for maintaining the content and integrity of the information at a European Level by diplomatic means.

2.1 Repositories

The Swedish CVCA maintains a repository containing the certificates and requests (CVCA certificates, CVCA link certificates, DV certificates and DV requests) as well as registration data of domestic and foregin DVs together with suspension status lists. The information is stored for the validity time of the corresponding certificate plus the validity time of the MRTDs the certificate are used by and adding six months.

The Swedish DV maintains a repository containing the certificates and requests (DV certificates, DV requests and IS certificates) as well as registration data of maintained Inspection Systems. The certificates in the DV repositories are stored for the validity time of the corresponding certificate plus one year)

3 Identification and Authentication

3.1 Naming

As defined in BSI-EAC, the Certification Authority Reference identifies the public key used for verifying the signature of the certification authority (CVCA or DV).

The Certificate Authority Reference is equal to the Certificate Holder Reference in the corresponding certificate of the certification authority (CVCA Link Certificate or DV Certificate).

The Certificate Holder Reference identifies a public key of the certificate holder. It is a unique identifier relative to the issuing certification authority. It consists of the following concatenated elements:

- 1) The ISO 3166-1 ALPHA-2 country code of Sweden;
- 2) A mnemonic that represents the certificate holder;
- 3) A numeric or alphanumeric sequence number.

NOTE: It is not guaranteed that the Certificate Holder Reference (CHR) is a unique identifier in general.

Sweden has defined identities as follow:

- CVCA certificate:
  - Certification Authority Reference: national CVCA identity
  - Certificate Holder Reference: national CVCA identity

- DV certificate:
  - Certification Authority Reference: national CVCA identity or other authorized Member State CVCA (see section **Fel! Hittar inte referenskälla.**) identity
  - Certificate Holder Reference: national DV identity

- IS certificate:
  - Certification Authority Reference: national DV identity
  - Certificate Holder Reference: national IS identity.

3.2 SE Naming Convention

The Country Code for the Sweden is SE .

For the Swedish DV, the Swedish Police Authority will be responsible for defining the mnemonic that represents the Certificate Holders.

The Swedish Certificate Practice Statement contains the full Naming Convention for DV certificates.

3.3 Registration

3.3.1 Domestic CVCA Initial Identity Validation

The Swedish Police Authority has stated who is responsible for the authentication and the definition of the identity of each CVCA and the National PKI Co-ordinator.

3.3.2 Registration of a foreign Member State

The Swedish CVCA registration is carried out under the supervision of the European Commission. The registration of the Swedish CVCA consists of two steps:

Step 1 Submitting registration via European Commission

Swedens's National PKI Co-ordinator submits the signed registration form (Appendix D Registration form) to the European Commission for distribution to other participating Member States by diplomatic means securing the authenticity and integrity of the information. In some cases, this part of the registration is done bilateral directly between Member States. In such cases, the European Commission is informed about the registration.

Step 2 Implementing registration information at domestic CVCA

The Swedish CVCA registration information is also distributed to the Member State's National PKI Co-ordinator and further to its CVCA and SPOC in a way that secures the authenticity and integrity of the data.

When receiving CVCA registration data from a foreign Member States, the Swedish National PKI Co-ordinator, the Swedish CVCA, and the national SPOC verifies that the integrity of the information has not been compromised. The digital certificate data of a foreginMember State's CVCA certificate and the SPOC root certificate are checked against the cryptographic fingerprints listed on the registration form of the corresponding Member State.

If these checks lead to a positive result, the registration data is implemented at the Swedish CVCA and hence the registration is completed by requesting all newer CVCA Certificates from the registered Member State via SPOC communication (GetCACertificates according to CSN-SPOC). If the check leads to a negative result, the registration data is rejected and the process has to be restarted.

In event of a change to any of the registration information above, the Swedish National PKI Co-ordinator submits the updated version to the European Commission for distribution to other participating Member States. Before performing an update of a registration the Registration Authority verifies if the integrity of the information has not been hurt.

The Swedish National PKI Co-ordinator informs Member State, having applied for being registered, if the registration has been accepted or rejected (including the reason) with in 4 weeks. This message is sent by Swedish National PKI Co-ordinators to the corresponding Member State.

3.3.3 Registration of a DV

The initial registration of a DV to the Swedish CVCA Registration Authority is done by the RA of the Swedish CVCA. This registration process contains checks for securing the identity of the DV, authenticity of registration data (including initial certificate request), audit certification, the DV s certificate policy, and if applicable, the public part of certificate practice statement and the permissions the DV have for applying for certificates.

If these checks lead to a positive result, the Swedish CVCA registers the DV and sign initial DV requests to foreign Member State's CVCA. If the check leads to a negative result, the DV registration is rejected and the process has to be restarted.

The registration of a foregin DV to the Swedish CVCA is done based on the known CHR of the DV and is finished by accepting the initial request of the DV signed by a known valid CVCA Certificate of the foregin CVCA.

Thereafter the Swedish CVCA lists the DV as valid and not suspended until a notification of an incident concerning the fulfilment of security requirements according to this CP or the termination of the DV is known.

3.3.4 Registration of an IS

The Swedish DV has proper mechanisms in place to identify an authenticated Inspection System. The key generation of an Inspection System is processed under consideration of sections 4.4.5, 5 and 6. The initial request of an IS is transmitted to the DV in a secure way. The DV checks if the integrity and authenticity of the request data is unhurt.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Profile

Swedish CVCA certificates, CVCA link certificates, DV certificates and IS certificates is produced according to the certificate profile specified in BSI-EAC CV Certificates .

4.2 Initial Certificates and Requests

An initial certificate of a DV or IS is defined as

being the first certificate of the same Certificate Holder or
being the first certificate after a suspension has been canceled or
being a new certificate after the previous certificate has been expired before a new request or link certificate could be generated.

An initial certificate of a Swedish DV or IS is issued based on an initial request of that DV or IS according to BSI-EAC.

Certificates are not issued without generating a new key pair for the corresponding certificate.

4.3 Successive Certificates and Requests (Re-key)

A successive certificate is every certificate of the same Certificate Holder (Subscriber) except an initial one (see above).

A successive certificate is issued only after conforming to the following rules:

a) A new key pair is generated by the Certificate Holder;
b) The certificate contains a different (successive) sequence number in the CHR than the previous certificate(s) of the Certificate Holder;
c) The certificate is issued in accordance with 4.4 Certificate Application and Issuing.
d) In case of a private key compromise, the cause for the incident is first detected and the corresponding security problem is then solved before issuing a new initial certificate (see chapter 4.2 Initial Certificates and Requests).

A successive certificate for a DV or IS is issued only after conforming to the following rules:

a) The DV or IS certificate is about to expire, in this case BSI-EAC chapter Certificate Requests follows.
b) When a certificate requires modification due to changes in the DV\IS attributes;

Certificates are not issued without generating a new key pair for the corresponding certificate.

4.4 Certificate Appliacation and Issuing

The Swedish Certificate Authorities (CVCA and DV) takes measures against the forgery of certificates and ensure that the procedure of issuing the certificate is securely linked to the associated registration.

4.4.1 Certificates issued by CVCA to CVCA

The Swedish Police Authority defines which entity is responsible to authorize the CVCA creation.

The CVCA only issue self signed CVCA certificates or a CVCA link certificates to a former CVCA certificates of the same CVCA[3]. This is done during a key ceremony which fulfills the security requirements in chapters 5 and 6 of this Swedish Certificate Policy. The Swedish CVCA checks that a certificate request is authorized and valid.

When the validity of a CVCA certificate is about to expire, the CVCA generates a new key pair and issue a self-signed CVCA certificate and a CVCA link certificate[4].

The CVCA link certificate contains:

the public key of the new key pair,
a signature generated with the private key of the previous CVCA certificate ,
the same validity period as the new CVCA certificate holding the same public key

according to BSI-EAC. The new CVCA certificate and the CVCA link certificate are distributed to all foreign Member States registered at the Swedish CVCA via SendCertificates message according to CSN-SPOC.

When receving a new CVCA certificate and a corresponding CVCA link certificate, the Swedish CVCA / SPOC checks the validity and authenticity of the certificate:

if the received certificate is correct according to syntax, authenticity and validity the Swedish CVCA updates its registration information of the foregin CVCA with CVCA certificate and CVCA link certificate as new trusted CVCA certificates;
if the certificate is not correct, the Swedish CVCA informs the issuing CVCA of the CVCA (link) certificate. This is done by responding to the SendCertificate message according to CSN-SPOC automatically.

[3] or a new CVCA being the replacement for a terminated CVCA according to chapter 5.4.
[4] The CVCA link-certificate will be used as part of the trusted path for the MRTDs to be read and to proof the authenticity of the new CVCA certificate and the self-signed CVCA certificate is used to proof the possession and operational reliability of the corresponding private key.

4.4.2 Certificates issued by CVCA to DV

Following successful registration as per 3.2.3 above, DV Certificate Application is carried out in accordance with BSI-EAC (chapters Certificate Requests and BSI-EAC Document Verifiers) as follows:

The DV certificate request contains the inner CAR (this is in BSI-EAC only recommended) in order to distinguish between the different foregin CVCAs. In Sweden there is only one CVCA receiving the certificate request.

4.4.3 Certificate application

The following steps are taken when a certificate shall beissued by a foreign Member State's CVCA to a Swedish DV:

Table 1: Generating and processing a DV Request

Step no.	Indication	Initial Request	Successive Request[5]	Party involved
1	**Generate key pair**	the DV generates a key pair according to BSI-EAC and in consideration of the security requirements of chapters 5 and 6 of this document;		DV
2	**Generate certificate request**	the DV generates a certificate request out of the new generated public key considering the naming scheme of chapter 3.1 and BSI-EAC and generates the inner signature (see BSI-EAC) with the corresponding private key;		DV
3	**Generate outer signature (successive request)**	-	The request MUST be signed with the private key corresponding to a still valid DV certificate which has been issued by the same Member State the request shall be sent to.[6]	DV
4	**Send Request to CVCA/ SPOC**	The request MUST be submitted to the corres-ponding domestic[7] CVCA of the DV in a secure way.	The signed request MUST be submitted to the domestic CVCA/SPOC.	DV

[5] Initial / Successive Request concerning the Member State's CVCA which shall sign the DV certificate.
[6] If a private CVCA, DV or IS key is unusable for non-critical reasons, as a delayed successive request, a new initial request SHALL be produced (see also chapter 5.3.3).
[7] Domestic/foreign means in the context of this table same/other Member State than the DV

Step no.	Indication	Initial Request	Successive Request[5]	Party involved
5	**Check suspension status (domestic)**	The domestic CVCA/SPOC MUST check if the DV is still allowed to request certificates from foreign Member States i.e. it is not suspended before processing the Request. A request of a suspended DV MUST be refused.		Domestic CVCA/ SPOC
6	**Check integrity**	The CVCA MUST check if the authenticity and integrity of the DV request is correct, otherwise the request MUST be refused.	It is RECOMMENDED to check the authenticity and integrity of the request within the CVCA/SPOC by automatic means.	Domestic CVCA/ SPOC
7	**Generate outer signature (initial request)**	An outer signature has to be added to the request by the corresponding domestic CVCA. Then forward the request to the domestic SPOC.	-	Domestic CVCA
8	**Submit request to foreign SPOC**	The request SHALL be submitted to the foreign SPOC following the requirements of CSN-SPOC.		Domestic SPOC
9	**Check outer signature**	The foreign SPOC/CVCA MUST check if the outer signature of the request is created with a key which is valid with respect to:		Foreign CVCA/ SPOC
		a still valid root certificate of the DV's domestic CVCA which is registered as valid at the foreign Member State's CVCA.	a still valid certificate of that DV, issued by the foreign Member State's CVCA itself.	
10	**Check suspension status (foreign)**	The foreign Member State's CVCA MUST check if the DV is still allowed to apply for certificates concerning the information provided by the DV's domestic CVCA or if the foreign Member State has suspended the DV itself, i.e. checking registration status of the DV.		Foreign CVCA/ SPOC
11	**Issue certificate?**	If both checks of the two previous steps lead to a positive result the foreign CVCA MUST generate a certificate corresponding to the received request. Otherwise the request MUST be rejected.		Foreign CVCA
12	**Send response**	The foreign Member State's SPOC sends a response message to the DV's domestic SPOC, containing either the DV certificate or the refusal of the certificate application.		Foreign SPOC

Step no.	Indication	Initial Request	Successive Request[5]	Party involved
13	**Check certificate**	The domestic SPOC checks the syntax of the certificate by automatic means and sends the result of this check as response to the foreign SPOC (see CSN-SPOC)		Domestic SPOC
14	**Forward response**	The domestic SPOC of the DV forwards the response of the Member State's CVCA to the DV		Domestic SPOC
15	**Implement certificate**	DV implements the certificate		DV

4.4.4 Application period and response time

The Swedish CVCA will process a certificate request within a timeframe of 7 days.

In the event that a Swedish CVCA system is non-operational for more than this time frame, Sweden will inform the subscribing domestic DV and foreign Member State CVCAs no later than 7 days before the loss of service, if planned, and as soon as reasonably possible in the event of an unplanned loss of service.

For getting a new DV certificate, 11 days are scheduled. If there is need for a fall back to communication via email, 3 additional days are considered.

This time frame has been calculated as follows:

the key ceremony and internal quality assurance(1/2 day)
generating the corresponding certificate request (1/2 day)
submitting the request to signing authority via domestic SPOC (1 day)
response time of signing authority (7 days)
getting the certificate via domestic SPOC (1 day)
import of the certificate (1 day)

If the kind of installation of a DV s infrastructure requires a greater amount of time for one of the steps above, the DV will increase the time frame for generating a new DV Certificate Request accordingly.

4.4.5 Certificates issued by DV to IS

Inspection Systems may submit certificate requests upon completion of successful registration as per 3.3.4 above.

The DV only issues a certificate to an IS that is compliant with BIS-EAC CCP and that is using the certificates in accordance with part 4.6 of this document.

Table 2: Generating and processing an IS Request

Step no.	Indication	Initial Request	Successive Request[8]	Party involved
1	**Generate key pair**	The IS generates a key pair according to BSI-EAC and in consideration of the security requirements of chapters 5 and 6 of this document.		Inspection System
2	**Generate certificate request**	The IS generates a certificate request out of the new generated public key considering the naming scheme of chapter 3.1 and BSI-EAC and generates the inner signature (see BSI-EAC) with the corresponding private key;		Inspection System
3	**Generate outer signature**	-	The request SHOULD contain an outer signature generated with the private key corresponding to a still valid IS certificate. If this mechanism is not used, then another mechanism of equivalent security MUST be used.	Inspection System
4	**Submit request**	The request MUST be submitted to the corresponding DV in a way ensuring any compromise of the authenticity or integrity of the request can be detected. E.g. by submitting a cryptographic fingerprint of the request via a different channel.	The request MUST be submitted to the DV.	Inspection System
5	**Check request**	The DV MUST check if the authenticity and integrity of the IS request is not compromised and if the request is conformant to BSI-EAC and chapter 3.1 of this CP;	The DV MUST check if the outer signature is correct and generated with the private key corresponding to a still valid IS certificate and if the request is conformant to BSI-EAC and chapter 3.1 of this CP;	DV
6	**Check registration status**	The DV MUST check if the IS is still allowed to request certificates i.e. the registration of the IS is not suspended.		DV
7	**Issue certificate ?**	The DV MAY issue a certificate corresponding to the request if the checks of the previous two steps lead to a positive result otherwise the IS request MUST be refused;		DV

[8] Initial / Successive Request concerning the Member State's CVCA which shall sign the DV certificate.

Step no.	Indication	Initial Request	Successive Request[8]	Party involved
8	**Send response**	The DV SHALL send a response message to the IS containing either the IS certificate or the refusal of the certificate application.		DV
9	**Implement certificate**	The IS implements the certificate.		IS

4.5 Certificate Acceptance

Self signed certificates issued by the Swedish CVCA are accepted by the entity responsible for the CVCA after its creation at the end of the key ceremony.

A DV or IS are deemed to have accepted a certificate upon its receipt.

4.6 Certificate Usage

Inspection System Certificates are used to enable read access to fingerprint biometrics stored on the MRTDs as indicated in the certificates only according to COUNCIL REGULATION (EC) No 2252/2004.

For a Member State CVCA, keys pairs and certificates are used for the following purpose:

The Swedish CVCA private key is used to sign CVCA certificates, CVCA link certificates and domestic and foreign DV certificates and DV certificate requests to be provided to foreign authorized Member State s CVCAs (see section 3.3);
CVCA certificate are used to verify signatures of domestic or foreign Member State DV certificates and CVCA link certificates issued by this CVCA and DV requests signed by this CVCA;
DV private keys are used to sign domestic IS certificates and successive DV requests;
DV certificates are used to verify signatures of IS certificates issued by this DV.

Note: Every Swedish DV and IS holds several key pairs (and certificates) in use at the same time as needing one key pair for each foreign Member State (including own domestic one) issuing MRTDs. The Swedish CVCA holds only one key pair in use at the same time, excluding the short interval needed for signing the CVCA link certificate.

The trusted certification path for a Swedish MRTD being read by an IS of an authorized foreign Member State is as follows:

Authorized foreign Member State IS certificate,
corresponding authorized foreign Member State DV certificate signed by the Swedish CVCA certificate corresponding to the MRTD and
consists of zero or more swedish CVCA link certificates completing a certificate chain up to the Swedish CVCA public key stored on the MRTD.

Certificates and paths of certificates are validated and interpreted by relying parties according to ISO 7816-4 and BSI-EAC.

4.7 Certificate Validity Periods

Operational periods for certificates as specified in point 5.5.1 of Commission Decision C(2006) 2909 of 28.06.2006:

Entity	Minimun Validity Period	Maximum Validity Period
CVCA certificate	6 months	3 years
Document Verifier certificate	2 weeks	3 months
Inspection System certificate	1 day	1 month

5 Security Requirements

5.1 Physical Controls

Each Swedish CVCA and DV ensures that it operates its services in a secure environment. This includes:

a) **Site location and construction:** The Swedish CVCA/DV are operated in a physically protected area.
b) **Physical access:** Access to the Swedish CVCA/DV is controlled and audited. Only authorised persons have physical access to the CVCA/DV environment.
c) **Media storage:** The storage media are protected against unauthorised or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
d) **Waste disposal:** Procedures for the disposal of waste are implemented in order to avoid unauthorised use, access, or disclosure of sensitive data.

5.2 Procedural Controls and System Access Management

Every Swedish CVCA and DV implements security measures in order to protect the authenticity, integrity and confidentiality of their data and the accurate functionality of its IT systems. A Security Concept is written for each Swedish CVCA and DV which:

lists any IT systems being part of the Certificate Authority, Registration Authority or SPOC, being directly connected to one of these or handles data for the registration or certification process;
describes any process being part of the tasks of a Swedish CVCA, DV or SPOC;
describes the roles needed (see below);
describes security measures and incident handling.

The following items are concerned:

Protection of the IT system: IT security mechanisms (e.g. firewalls, proxies, TLS) are implemented to protect the internal network domains from external network domains accessible by third parties. Each interface of the used IT system is considered for implementing appropriate security measures;
Trusted roles: Processes of the Swedish SPOC, CA and RA tasks are attached to trusted roles. The following roles are available: system administrator, auditor, RA operator and CA operator. This is realised by the Swedish Police Authority organisational measures as well as IT controls and includes user account management, auditing and timely modification or removal of access.
Separation of trusted roles: the IT system provides sufficient computer security controls for the separation of trusted roles. Distinct trusted roles are not adopted by the same person.

Access Control: authentication of roles is enforced by the IT system for system access. Access to data or functionalities is only granted to trusted roles allocated to the corresponding task.
Two person principle: Separation of duties is implemented for critical tasks by a two person principle.
Substitution concept: for the case of inactivity of personnel covering trusted roles the substitution is planned in a timly manner. Also, in case of substitution, a person does not have the possibility to cover separated roles.
Separated systems: communication between separated IT systems is secured against manipulation and access of third parties. IT systems are separated according to their need of availability, internet communication (e.g. SPOC) and confidentiality, integrity of data (e.g. CA).
Sensitive data: Sensitive data is protected against unauthorised access or modification by way of encryption, access restriction mechanism, and account management. Sensitive data is protected (e.g. using encryption and an authenticity/integrity protecting mechanism) when exchanged over networks which are not secure.
Suspension of subscribers: the Swedish CVCA and DV provide adequate mechanisms for suspension of registered subscribers (foreign CVCAs, DVs, and IS respectively). These mechanisms prevent the issuing of certificates or signing of certificate requests of suspended subscribers.
Logging: every modification of sensitive data is logged which includes private key operations as well as registration information and status. Sub-chapter 5.2.1 defines the details on the logging requirements.
Archival: archived records are kept for a period of time as appropriate for providing necessary legal evidence in accordance with the applicable legislation of the Swedish Gonvernment.
Personnel: IT systems are operated by qualified and experienced staff. Sub-chapter 5.2.2 defines the details on the personnel requirements.
Life-Cycle of security measures: security measures are updated regularly during the life-cycle of the PKI. Sub-chapter 5.2.3 defines the details on the life-cycle requirements.
Testing system: The Swedish SPOC operates a pre-production testing system which is constructed very similar to the real SPOC, registration and certification systems in order to test new security measures, software updates and interoperability with IT systems of foreign Member States;

For each IS a **Security Concept** is written which describes:
the type and structure of the IS,
every IT system being part or hosting parts of the IS,
the security measures and incident handling.

The following items are concerned for the Security Concept of an IS:

Protection of the IS: IT security mechanisms (e.g. firewalls, TLS, Anti-Virus Software) are implemented on each IT system being part or hosting parts of the IS[9]. Each interface of the used IT systems is considered for implementing appropriate security measures.

[9] The security mechanisms depend on type and structure of the IS.

Access Control: authentication of roles is enforced by the IT system for system access. Access to data or functionalities is only granted to trusted roles allocated to the corresponding task.
Separated systems: If applicable, the communication between separated IT systems is secured against manipulation and access of third parties. IT systems are separated according to their need of availability, internet communication and confidentiality, integrity of data.
Sensitive data: Sensitive data is protected against unauthorised access or modification. Sensitive data is protected (e.g. using encryption and an authenticity/integrity protecting mechanism) when exchanged over networks which are not secure.
Logging: Sub-chapter 5.2.1 defines the details on the logging requirements for IS.
Archival: archived records are kept for a period of time as appropriate for providing necessary legal evidence in accordance with the applicable legislation of the Swedish Government.
Personnel: Inspection Systems are operated and administrated by qualified and experienced staff. Subchapter 5.2.2 defines the details on the personnel requirements.

5.2.1 Logging

The Swedish SPOC, CVCA, DV and IS implements appropriate logging procedures to analyse and recognize any proper and improper use of its system within the EAC-PKI.
The SPOC, CVCA and DV ensure that:

Events to be logged: the following events are logged:
creation, use and destruction of **keys and certificates**,
creation and modification of **registration entries**;
all requests and reports relating to **incident notification and suspension** of registrations, as well as the resulting actions;
Logging mode: the precise time of the concerning event and if applicable the trusted role having triggered or executed the event is recorded;
Integrity and confidentiality: the confidentiality and integrity of current and archived records is maintained. Events are logged in a way that they cannot be easily deleted or destroyed (except for transfer to long-term media) within the time period they are required to be held;
Archival: The logs are archived at least until the next full audit according to chapter 7 Compliance Audit and Other Assessment has been completed. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site. Access to archives are restricted to authorized operators only.
Documentation: The specific events and data to be logged are documented;

IS fulfills the following requirements for logging:

Key management: an IS logs each key management event as generating and deleting private keys;
Certificate Management: an IS logs the issuing of certificate requests and if corresponding certificates are received;

Access control: an IS logs each attempt of getting access to the IS functionalities;
Protection: The log is protected against modification or deletion;
Audit trail: Records are kept to enable the auditor to confirm that misuse can be detected;
Prohibited logging: Inspection Systems does not log or transmit fingerprints obtained from MRTDs. Any traces of these biometrics are explicitly deleted immediately after finishing the comparison process between fingerprints acquired from the bearer and fingerprints read from the MRTD.

5.2.2 Personnel

The following requirements are maintained concerning personnel of the Swedish SPOC, CVCA, DV or IS:

Knowledge: Personnel possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function;
Reliability: Personnel undergo domestic security screening appropriate to the role(s) they are carrying out.
Conflicts of interest: Personnel are free from conflicts of interest;
Completing checks: Personnel have no access to the trusted functions until any necessary checks are completed;
Clear instructions: Personnel are clearly instructed on their duties and tasks;
Accountability: Personnel are accountable for their activities.

5.2.3 Life-Cycle of security measures

Security of the Swedish SPOC, CVCA, DV and IS is sustained by fulfilling the following requirements:

Searching for security news: Administrators and system developers search for news on security risks, attacks and countermeasures concerning the used hardware, software, algorithms and protocols at least once per month;
Up-to-date security: New security patches for software, algorithms or protocols are promptly implemented after being tested appropriately;
Closing gaps: Security measures are updated immediately if a security gap is known;
Change control: change control procedures are part of the Security Concept, and are documented, and used for releases, modifications and emergency software fixes for any operational software of the Swedish CVCA, DV and IS.
Security training: Personnel are trained on new security risks and countermeasures at least once every six months;
Retraining on duties: Personnel a retrained on duties and tasks at least once per year;
Review Security Concept: The Security Concept is reviewed, updated and compared with its realisation at least once per year;

5.3 Incident handling

5.3.1 Subscriber Suspension

Swedish CVCA, DV or IS will be suspended in case of:

any incidents as private key compromise or other security vulnerabilities being no longer conformant to this Swedish National Certificate Policy

Further, a Swedish DV or IS is also suspended if it is no longer allowed to apply for certificates of foreign Member States.

The suspension is processed by the Swedish SPOC, CVCA, and DV having registered the suspended CVCA, DV or IS.

5.3.2 Compromise and Disaster Recovery

Swedish CVCA take reasonable measures to ensure that continuity of service are maintained, including:

Measures to minimise the impact of disruption to power services;
Measures to minimise the impact of events such as flooding or fire;
Measures to minimise the impact of the loss of availability of key staff;

5.3.3 Incident and Compromise handling Procedures

Any Swedish CVCA, DV and IS ensure that in the event of a disaster, including compromise of the participant s private key, operations are restored as soon as possible. In particular, the following requirements hold:

Each Swedish CVCA, DV and IS define and maintain a continuity plan to enact in case of disaster.
Swedish CVCA and DV systems data necessary to resume CVCA and DV operations are backed up and stored in safe places suitable to allow the CVCA and DV to timely go back to operations in case of incident/disasters.
Back up and restore functions are performed by the relevant trusted roles.
The EAC-PKI business continuity plan (or disaster recovery plan) address the compromise or suspected compromise of a private key as a disaster and the planned processes are in place (see also Section 5.7.3).

If the private key of any Swedish CVCA, DV or IS is unusable for non-critical reasons, as a delayed successive request, a new initial request is produced as described in chapter 4.2 Initial Certificates and Requests.

If the private key of any Swedish CVCA, DV or IS is unusable for critical reasons as e.g. key compromise, the security problem having caused the compromise are solved first, before a new initial request is produced as described in chapter 4.2 Initial Certificates and Requests.

5.3.4 Entity Private Key Compromise Procedures

A Swedish DV immediately inform its National PKI Co-ordinator which informs all foreign Member State s National PKI Co-ordinators that have issued certificates for this DV about private key compromise or misuse. Domestic and foreign CVCAs will immediately suspend that DV.

Following suspension of a CVCA or DV certificate by the Swedish CVCA, the use of that private key is immediately and permanently discontinued.

If a Swedish IS is lost, stolen or its private key is compromised or control over the private key has been lost, the responsible Document Verifier is immediatally informed. The DV immediately suspends that IS in order to prevent the issuance of new certificates for this IS. In case of key compromise, which includes the possibility of unauthorized private key use on lost or stolen Inspection Systems, the Member States involved is informed.

Following suspension of an IS the use of a private key is immediately and permanently discontinued.

The incident information to foreign Member States is distributed via the Swedish SPOC and via the Swedish National PKI Co-ordinator using the wording of section C.4 Sending notifications.

The incident report and the solution of the security problem having caused the incident are shared with all Member States.

5.4 CVCA or DV Termination

In the event of a Swedish CVCA terminating its operations the following requirements are fulfilled:

Notification of foreign National PKI-Coordinators: the terminating Swedish CVCA notifies each registered foreign National PKI Co-ordinator of the termination and, if any, which new Swedish CVCA will take over its tasks;
Notification of European Commission: the European Commission is notified by the Swedish National PKI Co-ordinator about the termination of said CVCA;
Continuity of certificate path: The new CVCA will continue to provide certificates for MRTDs issued under the previous CVCA. Link certificate will be issued which contains the first public key of the new CVCA and is signed by a valid private key of the replaced CVCA;
Destruction of keys: The terminating CVCA will destroy, or withdraw from use, its private keys;

In the event of a DV terminating its operations are as follows:

Notify domestic CVCA: The terminating DV notifies the corresponding Swedish CVCA
Notify foreign CVCAs: The Swedish CVCA/SPOC of the DV notifies all foreign National PKI Co-ordinators the CVCA is registered at[10].
Suspend DV s registration: All notified domestic/foreign CVCAs must suspend the DV's registration for the further issuance of certificates.
Destruction of keys: The terminating DV must destroy, or withdraw from use, its private keys.

[10] For the case a DV has not yet got the first certificate from those CVCAs but has applied for one.

6 Key Pair Security

6.1 Key Pair Generation

Swedish CVCA and DV ensures that their keys are generated

in controlled circumstances according to Section 5 Management, Procedural and Physical Controls of this document;
within a cryptographic module which is compliant with Appendix B;
and distributed in accordance with BSI-EAC and this policy;
and the Swedish CVCA and DV ensure that the integrity and authenticity of their public keys and any associated parameters are maintained during distribution of DV and IS certificates.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private keys of Swedish CVCA, DV and IS are held and used adhering the following rules:

Trustworthy device: Private keys are held and used within a cryptographic module which is compliant with Appendix B Hardware Requirements and only leave the cryptographic module for back-up purposes according to 6.3 Key Escrow, Backup and Recovery.
Lifecycle of trustworthy device: The security of trustworthy devices are ensured throughout their lifecycle including ensuring that the cryptographic module is not tampered with during shipment or storage, functions correctly when in operation and any private keys stored on the equipment is destroyed upon module retirement.
Access control of trustworthy device: Where keys are stored in a cryptographic module, access controls are in place to ensure keys are not accessible outside the cryptographic module. Measures have been taken to prevent unauthorised use of private keys.
Key destruction: Private signing keys are never used beyond the end of their lifecycle and all copies of the key are destroyed or put beyond use at the end of their life.

6.3 Key Escrow, Backup and Recovery

If key back-up for CVCA or DV private keys is done, it is executed according the processes described in chapter 6.2 Private Key Protection and Cryptographic Module Engineering Controls in this Certificate Policy and the following rules:

Backup copies of the private key are stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The number of personnel authorised to carry out this function are kept to a minimum.

Backup copies of the private keys are protected in a way that ensures the same or greater level of protection as provided by the cryptographic module.
Backup copies of the private keys of the Swedish CVCA and DV are never used anywhere except for restoration of the service of the domestic cryptographic module.

Private keys of Swedish CVCA, DV or IS are not escrowed. Private keys of Swedish IS are not backed up, as shown in the following table:

	CVCA	**DV**	**IS**
Back-up	YES	YES	NO
Escrow	NO	NO	NO

If a private key of a Swedish DV or IS is unusable for non-critical reasons, the DV or IS generate a new key pair and request for a new certificate at its signing authority (see chapter 5.3.3).
Swedish CVCA private keys are backed up in order to secure the certificate chain needed to get read access to the MRTDs.

7 Compliance Audit and Other Assessment

Each Swedish CVCA and DV is audited according to the following requirements:

Auditor qualification (only DV): the Swedish DV selects an independently acting and accredited company/organisation ("Auditing Body") or certified auditors to audit the DV according to this Common Certificate Policy. The Auditing Body is either accredited for this purpose by its national accreditation body or authorised by a responsible government office.
Control by authority (CVCA and DV): the Security Concept, its realisation and the conformity to this Certificate Policy of Swedish CVCA and DV is controlled by a domestic authority.
Audit basis: The Audit is based on ISO/IEC 27001 and 27002.
Checking requirement realisation: The audit and control does not only check that procedural security controls are specified but also that they are adhered to in practice. This also includes the registration process, the receipt of the initial certificate request and the suspension procedure for Inspection Systems subscribing to the DV.
Iteration of audits and controls: Audits and controls are performed at least every three years. The Auditing Body and the controlling authority carry out a review at least once a year by a team of one or more auditors to ensure on going compliance with this CP.
Being not conformant: In the event that an audit indicates that a Swedish DV is not conformant to this Common CP, or its certification becomes invalid or expires, the DV notifies its domestic National PKI Co-ordinator which will notify all foreign Member State s National PKI Co-ordinators to suspend that DV for requesting certificates. The foreign Member States must not issue any further DV certificates to this DV.
Availability of audit results: The certificate of conformity MUST be made available to other Member States and the Commission.
Reuse of audit results: The conformity of the DV to the Swedish National Certificate Policy and its Certificate Practice Statement if applicable may also be proven by this audit, for this those documents have to be considered additionally.

It is RECOMMENDED that a DV implements an Information Security Management System (ISMS) for its CA and RA functionality in accordance to ISO/IEC 27001. The ISMS is based on an ISMS policy of which its scope is defined by the Common Certificate Policy and if applicable the associated Certificate Practise Statement.

The operational environment supporting the SE EAC-PKI is ISO 27001 accredited.

The SE EAC-PKI, comprising the CV, DV and SPOC is subject to annual reaccreditation activity, regarding Information Assurance risks. Further detail can be found in the Certification Practice Statement.

Appendix A - Definitions and Acronyms

Appendix A.1. Definitions

1. *Certification Authority* An entity that issue certificates

2. *Certificate Revocation List* A list of revoked certificates;

3. *Certificate Policy* A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirement;

4. *Certificate Practice Statement* A statement of the practise that a certification authority employs in issuing, managing, revoking and renewing or re-keying certificates;

5. *Common Certificate Policy* The outline Certificate Policy published by the Commission which sets the minimum requirements for Member States National Certificate Policies to meet, in order to be included within the EAC-PKI.

6. *Common Criteria* - Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

7. *Extended Access Control Public Key Infrastructure* The infrastructure required to control access to fingerprint biometrics on Passports and Travel Documents utilising Extended Access Control.

8. *Document Signer* the entity signing the original document, in this case the organisation that issues the MRTD;

9. *Document Verifier* an entity within the EAC-PKI that requests certificates from CVCAs and, on the basis of those certificates, issues certificates to Inspection Systems;

10. *Evaluation Assurance Level* a numeric grade assigned to an IT system or product following the completion of a Common Criteria security evaluation

11. *Inspection System* the operational system that reads fingerprint biometrics from MRTDs.

12. *International Civil Aviation Organisation* A UN organisation tasked with fostering the planning and development of international air transport. In this role it sets international standards for MRTDs

13. *Key ceremony* - A procedure whereby a key pair is generated using a cryptographic module and where the public key is certified.

14. *Link Certificate* Link certificates ensure business continuity without exchanging a new trusted self-signed root CVCA certificate out-of-band.

15. *Machine Readable Travel Document* An international travel document containing eye- and machine-readable data;

16. *National Certificate Policy* a Members States Certificate Policy for management of the process of issuing and receiving certificates too and from other Members States;

17. *National PKI Co-ordinator* Person or group of persons which is fully responsible for interacting with foreign Member States with respect to exchange of DV certificates and this Common Certificate Policy

18. *Object Identifier* a unique numerical sequence allowing a document to be identified;

19. *Public Part of the Certification Practice Statement* A subset of the provisions of a complete CPS that is made public by a CA

20. *Registration Authority* An entity that establishes enrolment procedures for certificate applicants, performs identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA

21. *Security Concept* A Security Concept is a documentation of all tasks, duties, involved personnel and IT-Systems, and the interfaces of IT-Systems of a CA/RA. Further a Security Concept describes in detail the countermeasures against threats and (organisational and technical) security measures to be realised.

22. *Single Point of Contact (SPOC)* Technical communication interface according to CSN-SPOC.

23. *Trusted certification path* A chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of one or more CVCA-certificates, link certificates as appropriate, a DV-certificate and the IS certificate.

Appendix A.2 Acronyms

CA	Certification Authority
CC	Common Criteria
CDP	Certificate Revocation List Distribution Point
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CV RA	Country Verifying Registration Authority
CSCA	Country Signing Certification Authority
CSPKI	Country Signing Public Key Infrastructure
CVCA	Country Verifying Certification Authority
EAC-PKI	Extended Access Control Public Key Infrastructure
DV	Document Verifier
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ICAO	International Civil Aviation Organisation
IS	Inspection System
MRTD	Machine-Readable Travel Document
OID	Object Identifier
RA	Registration Authority
SPOC	Single Point of Contact

Appendix B Hardware Requirements

The crypto modules used by certificate authorities SHALL be evaluated and certified in accordance with one of the following standards:

FIPS PUB 140-1 level 3 or higher [11]
FIPS PUB 140-2 level 3 or higher [12]
PP-SSCD [13,14,15]
BSI Cryptographic Modules Security Level Enhanced [16]

Appendix B.2 Requirements for Inspection Systems

Member States SHALL adopt security targets for their inspection systems in accordance with Section 6. The inspection system SHALL be evaluated at a minimum level 2 and the key management component SHALL be evaluated at Level 4, augmented by VLA4 or VAN5.

[11] Security Requirements for Cryptographic Modules (FIPS PUB 140-1).
[12] Security Requirements for Cryptographic Modules (FIPS PUB 140-2).
[13] BSI-PP-0004-2002T Protection Profile Secure Signature-Creation Device Type 1, Version 1.05
[14] BSI-PP-0005-2002T Protection Profile Secure Signature-Creation Device Type 2, Version 1.04
[15] BSI-PP-0006-2002T Protection Profile Secure Signature-Creation Device Type 3, Version 1.05
[16] BSI-PP-0036-2008: Cryptographic Modules Security Level "Enhanced" Version 1.01