Polisen
Swedish Police

Date
19th of November 2021

02.00

Registration number
A304.828/2021

Reference No
170

Swedish Police Authority
IT Department

POLISMYNDIGHETEN

National Certificate Policy (CP)

Extended Access Control Infrastructure for Travel and Residence Documents

2021-11-19

This document is the principal statement of policy governing the Country Verifying Certification Authority (CVCA) and Document Verify Certification Authority (DVCA) in the Kingdom of Sweden.

Author	Swedish Police Authority		
Publication date	01.12.2021		
Version	2.0		
Status	In Process	Under Review	Authorised for Use
	☐	☐	☒

Authorisation

Place and date:	**Stockholm, 19.11.2021**
Approved by:	**Swedish Police Authority**
Approval number:	**UTS-240/2021**

Version history

Version History			
Date	Version	Author	Remarks
19.12.2008	1.0	Gillis Fredholm	Initial Release of version 1
14.08.2018	1.6	Joakim Stenius	Update of version1
01.10.2021	2.0	Anders Nygren	Initial Release of version 2
19.11.2021	2.0		Approved

1 Introduction

This document is the principal statement of policy governing the Country Verifying Certification Authority (CVCA) and Document Verify Certification Authority (DVCA) in the Kingdom of Sweden.

The Certificate Policy (CP) sets forth the business, legal, and technical requirements for approving, issuing, managing, revoking, and renewing, digital certificates within the CVCA and provides associated trust services for all participants using compatible systems for machine readable travel documents with biometric personal data. These requirements facilitate the security and the integrity of the Swedish CVCA and thereby provide assurances of trust.

A CVCA is a non-public certification authority established to meet the obligation for securing control systems accessing sensitive personal data stored in eMRTD (electronic Machine Readable Travel Documents) with biometric elements.

The aim of a CVCA is to provide certification services for entities governing inspection systems, called DV (Document Verifiers).

The consumers of CVCA certification services are DVs in the Kingdom of Sweden and in other countries.

The Swedish CVCA is the only certification authority used for managing access to biometric elements in eMRTDs issued by the Kingdom of Sweden.

The [BSI-CCP] document with its matching paragraphs forms the basis of the national policy.

1.1 Definitions

As defined in [BSI-CCP]
Additionally;
“Domestic” is defined to mean the Kingdom of Sweden.

DVCA and DVRA will be assumed to be part of the DV and only the term DV will be used.

1.2 Overview

As defined in [BSI-CCP]

1.3 Document Name and Identification

The policy is identified by name, version and OID:

- National Certificate Policy (CP) Swedish Verifying CA
- Version 2.0
- OID 1.2.752.84.101.1.1

1.4 PKI Participants

As defined in [BSI-CCP]

1.4.1 National PKI Co-ordinator

As defined in [BSI-CCP]

The Swedish NPC is responsible for coordinating the operations of Swedish CVCA and DV.

1.4.2 Certification Authorities

As defined in [BSI-CCP]

1.4.3 Registration Authority

As defined in [BSI-CCP]

1.4.4 Subscribers

As defined in [BSI-CCP]

1.4.5 Relying Parties

As defined in [BSI-CCP]

1.4.6 SPOC – Communication between participants

As defined in [BSI-CCP]

1.5 Policy administration

Swedish Police Authority
Information Technology Department
National PKI Co-ordinator
Box 12256
SE – 106 75 Stockholm
Phone: +46 77 114 14 00
e-mail: emrtd@polisen.se

2 Publication and repository responsibilities

As defined in [BSI-CCP].

2.1 Repositories

As defined in [BSI-CCP].

3 Identification and Registration

3.1 Naming

As defined in [BSI-CCP]

3.2 Registration

3.2.1 Domestic CVCA Initial Identity Validation

As defined in [BSI-CCP]

3.2.2 Registration of a foreign Member State

As defined in [BSI-CCP]

3.2.3 Registration of a DV

As defined in [BSI-CCP]

3.2.4 Registration of an IS

As defined in [BSI-CCP]

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Profile

As defined in [BSI-CCP]

4.2 Initial Certificates and Requests

As defined in [BSI-CCP]

4.3 Successive Certificates and Requests (Re-key)

As defined in [BSI-CCP]

4.4 Certificate Application and Issuing

As defined in [BSI-CCP]

4.4.1 Certificates issued by CVCA to CVCA

As defined in [BSI-CCP]

4.4.2 Certificates issued by CVCA to DV

As defined in [BSI-CCP]

4.4.2.1 Certificate application

As defined in [BSI-CCP]

4.4.2.2 Application period and response time

As defined in [BSI-CCP]

4.4.3 Certificates issued by DV to IS

As defined in [BSI-CCP]

4.5 Certificate Acceptance

As defined in [BSI-CCP]

4.6 Certificate Usage

As defined in [BSI-CCP]

4.7 Certificate Validity Periods

As defined in [BSI-CCP]

5 Security Requirements

5.1 Physical Controls

As defined in [BSI-CCP]

5.2 Procedural Controls and System Access Management

As defined in [BSI-CCP]

5.2.1 Logging

As defined in [BSI-CCP]

5.2.2 Personnel

As defined in [BSI-CCP]
Additionally:

- All staff members working with the Swedish EAC-PKI must have security clearance in accordance with regulations at the Swedish Police Authority.
- Operators of CVCA, DV and eMRTD-Biometric Extraction must be organisationally located within the Travel document systems group (Resehandlingssystem).

5.2.3 Life-Cycle of security measures

As defined in [BSI-CCP]

5.3 Incident Handling

Incidents shall be reported in accordance with routines at the Swedish Police Authority.

5.3.1 Subscriber Suspension

As defined in [BSI-CCP]

5.3.2 Compromise and Disaster Recovery

As defined in [BSI-CCP]

5.3.3 Incident and Compromise Handling Procedures

As defined in [BSI-CCP]

5.3.4 Entity Private Key Comproise Procedures

As defined in [BSI-CCP]

5.4 CVCA or DV Termination

As defined in [BSI-CCP]

6 Key Pair Security

6.1 Key Pair Generation

As defined in [BSI-CCP]

6.2 Private Key Protection & Cryptographic Module Engineering Controls

As defined in [BSI-CCP]

6.3 Key Escrow, Backup and Recovery

As defined in [BSI-CCP]

7 Compliance Audit and Other Assessment

As defined in [BSI-CCP] but with the following deviation (marked below) in *italics*.

The Swedish CV and DV are operated by the Swedish Police Authority with regulated access to both premises as well as documentation. The consequence is that an external auditing body will not be able to perform neither audit nor controls and because of this, these tasks are conducted by the internal IT Security Group. The IT Security Group is operated independently within the IT Department of the Swedish Police Authority.

CV and each DV SHALL be audited according to the following requirements:

- ***Auditor qualification:*** *Auditing Bodies MUST be authorised by the Swedish Police Authority.*
- ***Control by authority:*** *the Security Concept, its realisation and the conformity to this CP SHALL be controlled by the IT Security Group of the Swedish Police Authority.*

8 References

As defined in [BSI-CCP] References
Additionally:

BSI-CCP	Common Certificate Policy for the Extended Access Control Infrastructure for Travel and Residence Documents issued by EU Member States BSI TR-03139 version 2.2 of 31. July 2018

9 Appendix A Definitions and Acronyms

9.1 A.1 Definitions

As defined in [BSI-CCP]

9.2 A.2 Acronyms

As defined in [BSI-CCP]

10 Appendix B Hardware Requirements

As defined in [BSI-CCP]

11 Appendix C SPOC Requirements

As defined in [BSI-CCP]

11.1 C1. SPOC Initial registration

As defined in [BSI-CCP]

11.2 C2. SPOC CA requirements

As defined in [BSI-CCP]

11.2.1 C.2.1 Certificate assurance and content

As defined in [BSI-CCP]

11.2.2 C.2.2 Certificate revocation information

As defined in [BSI-CCP]

11.2.3 C.2.3 Technical and organizational requirements

As defined in [BSI-CCP]

11.2.4 C.2.4 Validity periods

As defined in [BSI-CCP]

11.2.5 C.2.5 Distribution of successive SPOC root certificates

As defined in [BSI-CCP]

11.3 C.3 Communication priorities

As defined in [BSI-CCP]

11.4 C.4 Sending notifications

As defined in [BSI-CCP]

12 Appendix D Registration form

As defined in [BSI-CCP]

12.1 D.1 Registration form commentary

As defined in [BSI-CCP]

12.2 D.2 Registration form sheets

As defined in [BSI-CCP]

13 Member State Registration Information

13.1 Part I - Member State (National PKI Co-ordinator)

As defined in [BSI-CCP]

13.2 Part II – SPOC Root Certificate and URL

As defined in [BSI-CCP]

13.3 Part III – CVCA Certificate

As defined in [BSI-CCP]