Swedish Police Authority
IT Department
Joakim Stenius

POLISMYNDIGHETEN

SE Master List Policy

Joakim Stenius

2022-09-01

This document is the policy statement for the Swedish Master List of CSCA certificates created by the Swedish Police Authority and signed with the Swedish Police Authority's Master List Signer.

1 Introduction 3
1.1 Definitions 4
1.2 Assumptions 4
1.3 Document Name and Identification 4
1.4 Policy administration 4
2 Background 5
3 Swedish Master List Creation 6
3.1 CSCA Source 6
3.2 CSCAs for the Master List – Selection 6
3.3 Master List Creation and Signing 6
4 Swedish Master List Distribution 7
5 Master List and Certificate Revocation List (CRL) 8
5.1 Swedish Master List CRL Policy 8
6 CSCA Mater List Signing Certificate 9
6.1 Certificate Profile 9

Version history

Version	Description
1.0	Initial release of version 1

1 Introduction

The International Civil Aviation Organization (ICAO) Public Key Infrastructure (PKI) scheme for the electronic Machine Readable Travel Document (eMRTD) application, defined in ICAO Doc 9303 Part 12, specifies a two-layer certificate chain that enables an inspection system to verify the authenticity and integrity of the data stored in the eMRTD contactless chip. The (highest level) root Certificate Authority (CA) in this scheme is the Country Signing CA (CSCA), which authorises Document Signer Certificates (DSC) to digitally sign the Document Security Object (SOD) on the contactless chip. Certificates are distributed to relying States using the distribution methods described in Doc 9303 (Section 5 of Part 12).

[R1] ICAO Doc 9303, "Machine Readable Travel Documents", specifies that the primary mechanism for CSCA certificate distribution is bilateral exchange while distribution using Master Lists (ML) is supported as a secondary mechanism:

"*A Master List is a digitally signed list of the CSCA certificates that are "trusted" by the receiving State that issued the Master List. CSCA self-signed Root certificates and CSCA Link certificates may be included in a Master List. The structure and format of a Master List is defined in Section 8. Publication of a Master List enables other receiving States to obtain a set of CSCA certificates from a single source (the Master List issuer) rather than establish a direct bilateral exchange agreement with each of the issuing authorities or organizations represented on that list*"

(ICAO Doc 9303 Part 12, section 5.3)

The ML approach described in [R1] aims to provide a convenient mechanism of distributing and publishing one or more issuing States' CSCA Public Keys electronically, albeit that it does not replace bilateral diplomatic exchange as the favoured approach.

This document sets out the conditions and policy for the creation of a master list that will be signed by the Swedish eMRTD Master List Signer (MLS) and made publicly available.

1.1 Definitions

CA	Certification Authority.
CSCA	Country Signing Certification Authority.
CRL	Certificate Revocation List.
LDAP	Lightweight Directory Access Protocol.
ML	Master List. A countersigned list of received and validated CSCA certificates.
MLS	Master List Signer. The entity that signs a ML.
eMRTD	Electronic Machine Readable Travel Document.
ICAO	The International Civil Aviation Organization is a UN specialized agency in charge of the planning and the development of safe international civil air transport by adopting standards and recommended practices.
ICAO 9303	ICAO Specifications for eMRTD.
NPC	National PKI Co-ordinator.
NPKD	National Public Key Directory.
PKD	Public Key Directory. A central LDAP repository for eMRTD certificates operated by ICAO.

1.2 Assumptions

It is assumed that the reader is familiar with the concepts and mechanisms offered by public key cryptography and public key infrastructures.

It is assumed that the reader is familiar with the contents of [R1], ICAO Doc 9303, “Machine Readable Travel Documents “, [R2], ICAO Supplement to Doc 9303 and any other official documents issued by ICAO regarding Machine Readable Travel Documents

1.3 Document Name and Identification

The policy is identified by name and version:

- Swedish Master List Policy
- Version 1.0

1.4 Policy administration

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

2 Background

[R1] ICAO Doc 9303, “Machine Readable Travel Documents “, used to specify that the exchange of CSCA certificates had to be bilateral, without providing detailed specifications on mechanisms for this exchange. In the early years of e-passports, the lack of such specifications led to wide interpretation and inefficient processes for bilateral exchange between states.

For this purpose, ICAO later adopted a mechanism (Master List), which aims to provide means to electronically distribute and publish CSCA certificates. The approach is based on countersigning the CSCA certificates received from other foreign states onto a Master List, and distributing the list via ICAO PKD to support bilateral distribution between issuing states.

For this purpose, the countersigning state publishes a signed list of received and validated self-signed CSCA certificates. The process of countersigning keys issued by other CAs is also known as “Cross Certification” but, as opposed to X.509 Cross Certification in this application, no assertion is made by the countersigning state other than the fact that the countersigning state has received the CSCA certificate from the originating state.

With this as a background, Sweden employs a National Public Key Directory (NPKD) for storing certificates. The directory is accessed through an admin interface application using certificate-based access credentials. Further, the Swedish NPKD regularly connects to ICAO PKD to upload and download (1) certificates (2) certificate revocation lists, and (3) master lists.

3 Swedish Master List Creation

3.1 CSCA Source

All CSCA certificates that are to be included in the Swedish ML MUST

- be verified through direct communication with the issuing country (e.g. via bilateral exchange) or,
- be obtained by other means and verified using link certificates against previously established trust or,
- be obtained from multiple sources that include solid paperwork, ensuring beyond reasonable doubt that the certificate is genuine and valid or,
- be obtained via ICAO ML or,
- be obtained via Schengen ML

3.2 CSCAs for the Master List – Selection

a) Only certificates imported in the Swedish NPKD may be included in the Swedish ML*
b) Any certificate that is rejected by the Swedish CSCA prior to the import to the Swedish NPKD must not be included on the Swedish ML

Procedures outlined in a CSCA Import Ceremony document MUST be followed in order to assure adherence to the responsibilities of the issuing authority with regard to MLs outlined in Doc 9303:

"Before issuing a Master List the issuing Master List Signer SHOULD extensively validate the CSCA certificates to be countersigned, including ensuring that the certificates indeed belong to the identified CSCAs. The procedures used for this out-of-band validation SHOULD be reflected in the published certificate policies of the CSCA that issued the Master List Signer certificate."

* Upon successful verification, CSCA certificates obtained according to 3.1 are imported to the Swedish NPKD system.

3.3 Master List Creation and Signing

CSCA certificates and their corresponding Link Certificates taken from the Swedish NPKD, may be included in the Swedish ML.

An MLS certificate will be issued by the Swedish eMRTD-PKI group following a request from the NPC. The MLS certificate, together with the private key, will be store in a secure PKI environment. The Swedish NPC will initiate the creation of a new Swedish ML.

New Swedish MLs will be issued with approximately quarterly intervals when appropriate (i.e. due to the availability of new CSCA certificates)

4 Swedish Master List Distribution

The Swedish Master List may be distributed using some or all of following the methods:

- Hand delivered by the Swedish NPC
- Uploaded to ICAO PKD
- E-mail: from emrtd@polisen.se or csca.sweden@polisen.se
- Via the public download site at https://www.polisen.se

When distributing the Swedish ML, the following extract from [R1] will be clearly presented.

"Use of a Master List does enable more efficient distribution of CSCA certificates for some receiving States. However a receiving State making use of Master Lists MUST still determine its own policies for establishing trust in the certificates contained on that list"

(ICAO Doc 9303 Part 12, 5.3)

By distributing the Swedish ML, the Swedish CSCA provides a service. It does not assert that the certificates contained within the Swedish ML are trusted, only that due diligence has been performed by the Swedish CSCA in the creation of the Swedish ML as described in this document.

5 Master List and Certificate Revocation List (CRL)

The CRL is critical for the correct application of Passive Authentication. It is not the responsibility of the Swedish CSCA to ensure that other states receiving the Swedish ML has access to CRLs for all of the states whose CSCAs are contained in the Swedish ML.

5.1 Swedish Master List CRL Policy

CSCAs for states where the Swedish CSCA does not have access to the current CRL (or where such CRL has not been made available) may be included in the Swedish ML.

It is up to the state receiving and using the Swedish ML and its contents to determine its own policy with regards to accepting a CSCA for which they do not have access to the corresponding CRLs.

6 CSCA Mater List Signing Certificate

6.1 Certificate Profile

The Swedish MLS certificate will be rekeyed approximately every 12 months. In order to assure availability of the MLS certificates at all times, the MLS certificate will have a validity period of 15 months. The Private Key Usage Period will be 13 months.

7. References

[R1] ICAO Doc 9303, “Machine Readable Travel Documents “

[R2] ICAO Supplement to Doc 9303