



ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2021

Part 12: Public Key Infrastructure for MRTDs



Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION **Documents**
AVA Document Sharing Hub



| ICAO

Doc 9303

Machine Readable Travel Documents

Eighth Edition, 2021

Part 12: Public Key Infrastructure for MRTDs

Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION



Documents

Document Sharing Hub

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Downloads and additional information are available at www.icao.int/security/mrtd

Doc 9303, *Machine Readable Travel Documents*
Part 12 — *Public Key Infrastructure for MRTDs*
Order No.: 9303P12
ISBN 978-92-9265-422-1 (print version)

© ICAO 2021

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, without prior permission in writing from the International Civil Aviation Organization.

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue*; the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

AMENDMENTS		
No.	Date	Entered by

CORRIGENDA		
No.	Date	Entered by

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of ICAO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

TABLE OF CONTENTS

1. SCOPE	1
2. OVERVIEW OF THE PUBLIC KEY INFRASTRUCTURE	1
3. ROLES AND RESPONSIBILITIES.....	3
3.1 eMRTD PKI	3
3.2 Authorization PKI.....	6
4. KEY MANAGEMENT	9
4.1 eMRTD PKI	9
4.2 Authorization PKI.....	16
5. DISTRIBUTION MECHANISMS	18
5.1 PKD Distribution Mechanism	20
5.2 Bilateral Exchange Distribution Mechanism.....	21
5.3 Master List Distribution Mechanism	21
6. PKI TRUST AND VALIDATION	22
6.1 eMRTD PKI	22
6.2 Authorization PKI.....	25
7. CERTIFICATE AND CRL PROFILES	25
7.1 eMRTD PKI	25
7.2 Authorization PKI.....	38
8. SPOC PROTOCOL	46
8.1 SPOC Related Structures.....	47
8.2 SPOC Protocol Messages	48
8.3 Web Service	53
9. CSCA MASTER LIST STRUCTURE.....	59
9.1 SignedData Type	59
9.2 ASN.1 Master List Specification	60
10. Deviation List Structure.....	61
10.1 SignedData Type	61
10.2 ASN.1 Specification	63

	<i>Page</i>
11. REFERENCES (NORMATIVE).....	65
APPENDIX A TO PART 12. LIFETIMES (INFORMATIVE)	App A-1
A.1 Example 1.....	App A-1
A.2 Example 2.....	App A-1
A.3 Example 3.....	App A-2
APPENDIX B TO PART 12. CERTIFICATE AND CRL PROFILE REFERENCE TEXT (INFORMATIVE).....	App B-1
APPENDIX C TO PART 12. EARLIER CERTIFICATE PROFILES (INFORMATIVE).....	App C-1
APPENDIX D TO PART 12. RFC 5280 VALIDATION COMPATIBILITY (INFORMATIVE)	App D-1
D.1 Steps Relevant to eMRTD	App D-1
D.2 Steps Not Required by eMRTD	App D-5
D.3 Modifications required to process CRLs	App D-6
APPENDIX E TO PART 12. LDS2 EXAMPLE (INFORMATIVE).....	App E-1

1. SCOPE

Part 12 of Doc 9303 defines the Public Key Infrastructure (PKI) for the eMRTD application. Requirements for issuing States or organizations are specified, including operation of a Certification Authority (CA) that issues certificates and Certificate Revocation Lists (CRLs). Requirements for receiving States and their Inspection Systems validating those certificates and CRLs are also specified.

The Eighth Edition of Doc 9303 incorporates the specifications for Visible Digital Seals (known as VDS) and for the optional Travel Records, Visa Records and Additional Biometric Applications (known as LDS2) as an extension of the mandatory eMRTD application (known as LDS1).

Doc 9303-12 shall be read in conjunction with:

- Doc 9303-10 — *Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)*;
- Doc 9303-11 — *Security Mechanisms for MRTDs*; and
- Doc 9303-13 — *Visible Digital Seals*.

2. OVERVIEW OF THE PUBLIC KEY INFRASTRUCTURE

The eMRTD Public Key Infrastructure (PKI) enables the creation and subsequent verification of digital signatures on eMRTD objects, including the Document Security Object (SO_D) to ensure the signed data is authentic and has not been modified. Revocation of a certificate, failure of the certification path validation procedure or failure of digital signature verification does not on its own cause an eMRTD to be considered invalid. Such a failure means that the electronic verification of the integrity and authenticity of the LDS data has failed and other non-electronic mechanisms could then be used to make that determination as part of the overall inspection of the eMRTD.

The eMRTD PKI is much simpler than more generic multi-application PKIs such as the Internet PKI defined in [RFC 5280]. In the eMRTD PKI, each issuing State/Authority establishes a single Certification Authority (CA) that issues all certificates directly to end-entities, including Document Signers. These CAs are referred to as Country Signing Certification Authorities (CSCAs). There are no other CAs in the infrastructure. Receiving States establish trust directly in the keys/certificates of each issuing State or organization's CSCA.

The eMRTD PKI is based on generic PKI standards including [X.509] and [RFC 5280]. Those base PKI standards define a large set of optional features and complex trust relationships among CAs that are not relevant to the eMRTD application. A profile of those standards, tailored to the eMRTD application, is specified in this part of Doc 9303. Some of the unique aspects of the eMRTD application include:

- there is precisely one CSCA per issuing State;
- certification paths include precisely one certificate (e.g. Document Signer);
- signature verification must be possible 5-10 years after creation;
- CSCA name change is supported; and
- CSCA Link certificates are not processed as intermediate certificates in a certification path.

For the most part, the eMRTD PKI infrastructure is compliant with [RFC 5280]. However, the fact that CSCAs can undergo a name change imposes unique requirements on the eMRTD PKI that are incompatible with some of the CRL validation procedures defined in [RFC 5280]. These differences have been kept to a minimum and are clearly identified.

For VDS and LDS2, the Digital Signature PKI, which provides integrity and authenticity of the data objects, is an extension of the LDS1 PKI. The Signers for VDS and LDS2 are issued by the same CSCA which issues Signers for LDS1. The changes to the Certificate Profiles for these new applications are specified in this document. Taken together, this infrastructure is referred to as the **eMRTD PKI**.

The Digital Signature PKI consists of the following entities:

- Country Signing CA (CSCA);
- Document Signer Certificates (DSC) which is used to sign the Document Security Objects (SO_D);
- LDS2 Signer Certificates, which consists of the following:
 - LDS2-TS Signer – signs LDS2 Travel Stamps;
 - LDS2-V Signer – signs LDS2 Electronic Visas; and
 - LDS2-B Signer – signs LDS2 Additional Biometrics;
- Bar Code Signer Certificates (BCSC), for which the following two specific types are defined in this document:
 - Visa Signer Certificates (VSC); and
 - Emergency Travel Document Signer Certificates (ESC);
- Master List Signer Certificates (MSC) used to sign Master Lists;
- Deviation List Signer Certificates (DLSC) used to sign Deviation Lists; and
- Certificate Revocation List (CRL).

All the different certificate types are signed by the same CSCA. The CSCA also signs the CRL, which contains any revoked certificate irrespective of the type of certificate. All the certificates issued under the CSCA are collectively referred to as **Signer Certificates**.

For LDS2 applications, a separate **Authorization PKI** is defined. The Authorization PKI enables the eMRTD issuing State or organization to control and manage the foreign States that are given authorization to write LDS2 data objects to their eMRTDs and to read those data objects. A foreign State intending to read or write LDS2 data must obtain an authorization certificate directly from the eMRTD issuing State or organization.

The Authorization PKI uses a different certificate structure (ISO 7816 card verifiable certificates) and therefore requires additional infrastructure components.

LDS2 requires the terminal to prove to the eMRTD contactless IC that it is entitled to write LDS2 data objects to the contactless IC or that it is entitled to read LDS2 data objects. Such a terminal is equipped with at least one private key and the corresponding Terminal Certificate, encoding the terminal's public key and access rights. After the terminal has proven knowledge of this private key, the MRTD chip grants the terminal access to read/write LDS2 data as indicated in the Terminal Certificate.

The LDS2 authorization PKI consists of the following entities:

- Country Verifying CAs (CVCAs);
- Document Verifiers (DVs);
- Terminals; and
- Single Point of Contact (SPOC).

Distribution and management of the authorization certificates between CVCAs in one State and DVs in other States is handled through a Single Point of Contact (SPOC) in each State.

This Part 12 of Doc 9303 specifies the eMRTD PKI profile, the Authorization PKI profile and corresponding objects including:

- roles and responsibilities of entities in the infrastructure;
- cryptographic algorithms and key management;
- certificate and CRL content;
- certificate and CRL distribution mechanisms; and
- certification path validation.

3. ROLES AND RESPONSIBILITIES

This section details the entities and the roles and responsibilities of both the eMRTD PKI and the Authorization PKI.

3.1 eMRTD PKI

The authenticity and integrity of data stored on eMRTDs is protected by Passive Authentication. This security mechanism is based on digital signatures and consists of the following PKI entities for eMRTD PKI:

- **Country Signing CA (CSCA):** Each issuing State/Authority establishes a single CSCA as its national trust point in the context of eMRTDs. The CSCA issues public key certificates for one or more (national) Document Signers and optionally for other end-entities such as Master List Signers and Deviation List Signers. The CSCA also issues periodic Certificate Revocation Lists (CRL) indicating whether any of the issued certificates have been revoked.
- **Document Signers (DS):** A Document Signer digitally signs data to be stored on eMRTDs; this signature is stored on the eMRTD in a Document Security Object.
- **LDS2 Signers:** An LDS2 Signer digitally signs LDS2 data objects of one or more types.

- **Bar Code Signer (BCS):** A Bar Code Signer digitally signs the data (header and message) encoded in the bar code. The signature is also stored in the bar code. This document specifies two use cases for the use of Bar Code Signer, viz. Visa and Emergency Travel Documents.
- **Inspection Systems (IS):** An Inspection System verifies the digital signature, including certification path validation to verify the authenticity and integrity of the electronic data stored on the eMRTD as part of Passive Authentication.
- **Master List Signers:** A Master List Signer is an optional entity that digitally signs a list of CSCA certificates (domestic and foreign) in support of the bilateral distribution mechanism for CSCA certificates.
- **Deviation List Signers:** Deviation List Signers are used to sign Deviation Lists. Deviation lists are defined in Doc 9303-3.

The secure facilities to generate key pairs SHALL be under the control of the issuing State or organization. Each key pair includes a “private” key and a “public” key. The private keys and associated systems or facilities SHALL be well protected from any outside or unauthorized access through inherent design and hardware security facilities.

While the CSCA certificate remains relatively static, a large number of Document Signer certificates will be created over time.

The CSCA of each issuing State or organization acts as the trust point for the receiving State. The issuing State or organization distributes its own CSCA public key to receiving States in the form of a certificate. The receiving State establishes that this certificate (and certified key) are “trusted” through out-of-band means, and stores a “Trust Anchor” for that trusted key/certificate. These CSCA certificates SHALL be self-signed certificates issued directly by the CSCA. CSCA certificates MUST NOT be subordinate or cross certificates in a larger PKI infrastructure. CSCA self-issued link certificates may also be issued to help the receiving State in establishing trust in a new CSCA key/certificate following a key-rollover.

Note.— In some States there is a requirement that a centralized Controller of Certification Authority (CCA) be the supreme authority to publish self-signed certificates for all applications. In these cases, a possible solution is for the CSCA to create a self-signed certificate (satisfying the ICAO Doc 9303 requirements) and have that certificate countersigned by the CCA (satisfying the State’s own CCA requirement). However, these countersigned certificates are not part of the eMRTD PKI and would not be distributed to receiving States.

3.1.1 Country Signing Certification Authority

It is RECOMMENDED that CSCA key pairs (KP_{UCSCA} , KP_{RSCA}) be generated and stored in a highly protected, off-line CA infrastructure.

The CSCA private key (KP_{RSCA}) is used to sign Document Signer certificates (C_{DS}), other certificates and CRLs.

Country Signing Certification Authority certificates (C_{CSCA}) are used to validate Document Signer certificates, Master List Signer certificates, Deviation List Signer certificates, CRLs and other certificates issued by the CSCA.

All certificates and CRLs MUST comply with the profiles specified in Section 7 and MUST be distributed using the distribution mechanisms as specified in Section 5.

For PKD participants, each CSCA certificate (C_{CSCA}) MUST also be forwarded by the certificate issuer to the PKD (for the purpose of validation of Document Signer certificates (C_{DS})).

CRLs MUST be issued on a periodic basis as specified in Section 4.

3.1.2 Document Signers

It is RECOMMENDED that Document Signer key pairs (K_{PuDS} , K_{PrDS}) be generated and stored in a highly protected infrastructure.

The Document Signer private key (K_{PrDS}) is used to sign Document Security Objects (SO_D).

Document Signer certificates (C_{DS}) are used to validate Document Security Objects (SO_D).

Each Document Signer certificate (C_{DS}) MUST comply with the certificate profile defined in Section 7 and MUST be stored in the contactless IC of each eMRTD that was signed with the corresponding DS private key (see Doc 9303-10 for details). This ensures that the receiving State has access to the Document Signer certificate relevant to each eMRTD.

Document Signer certificates of PKD participants SHOULD also be forwarded by the certificate issuer to ICAO for publication in the ICAO Public Key Directory (PKD).

3.1.3 LDS2 Signers

An LDS2 Signer digitally signs LDS2 data objects of one or more types.

Where there is a need to refer to an LDS2 Signer as one that signs a particular LDS2 data object type, it is referred to as follows:

- LDS2-TS Signer – signs LDS2 Travel Stamps;
- LDS2-V Signer – signs LDS2 Electronic Visas; and
- LDS2-B Signer – signs LDS2 Additional Biometrics.

It is RECOMMENDED that each State have no more than one LDS2-TS Signer, one LDS2-V Signer and one LDS2-B Signer. It is also possible for one LDS2 Signer to combine some or all of these roles.

If further differentiation is required, such as the location at which a travel stamp was added, the individual officer who cleared a traveler, which officer granted a visa, or the location at which additional biometrics were added, it can be included in a proprietary field within the respective LDS2 data object itself.

3.1.4 Bar Code Signers

It is RECOMMENDED that Bar Code Signer key pairs (K_{PuBCS} , K_{PrBCS}) be generated and stored in a highly protected infrastructure.

The Bar Code Signer private key (K_{PrBCS}) is used to sign the data (header and message) encoded in the bar code. The signature is also stored in the bar code.

Bar Code Signer certificates (C_{BCS}) are used to validate the data (header and message) encoded in the bar code.

Each Bar Code Signer certificate (C_{BCS}) MUST comply with the certificate profile defined in Section 7. The Bar Code Signer Certificates are not contained in the digital seal itself. Hence, a country that issues documents protected with digital seals MUST publish all its Bar Code Signer Certificates. The primary distribution channel for Bar Code Signer Certificates is PKD/bilateral. Other mechanisms, e.g. publication on a website, are secondary channels.

Bar Code Signer certificates of PKD participants SHOULD also be forwarded by the certificate issuer to ICAO for publication in the ICAO Public Key Directory (PKD).

The Visa Signer (VS) and Emergency Travel Document Signer are special cases of the Bar Code Signer.

3.1.5 Inspection System

Inspection Systems perform Passive Authentication to ensure the integrity and authenticity of the data stored on the eMRTD contactless IC. As part of that process, Inspection Systems MUST perform certification path validation as indicated in Section 6.

3.1.6 Master List Signer

The Master List Signer private key is used to sign CSCA Master Lists.

Master List Signer certificates are used to validate CSCA Master Lists.

3.1.7 Deviation List Signer

The Deviation List Signer private key is used to sign Deviation Lists.

Deviation List Signer certificates are used to validate Deviation Lists.

3.2 Authorization PKI

The LDS2 application is written to the contactless IC of an eMRTD, by the Issuing State or organization at the time of personalization.

Before another State can write LDS2 objects to that contactless IC, it MUST obtain authorization from the Issuing State or organization to do so. Each LDS2 data object is digitally signed by an LDS2 Signer in the writing State and subsequently written to the contactless IC by an authorized terminal in that writing State. The two-step process of signing by a signer and writing by an authorized terminal is similar to the LDS1 concept where the Document Signer digitally signs Document Security Objects but they are subsequently written to the contactless IC through the personalization process, as illustrated in Figure 1. Subsequent reading of LDS2 objects from the contactless IC is done through terminals authorized for LDS2 reading of the LDS2 object type in question.

The authorization PKI enables the eMRTD Issuing State or organization to control access (read and write) to LDS2 data on contactless ICs in eMRTDs it issues.

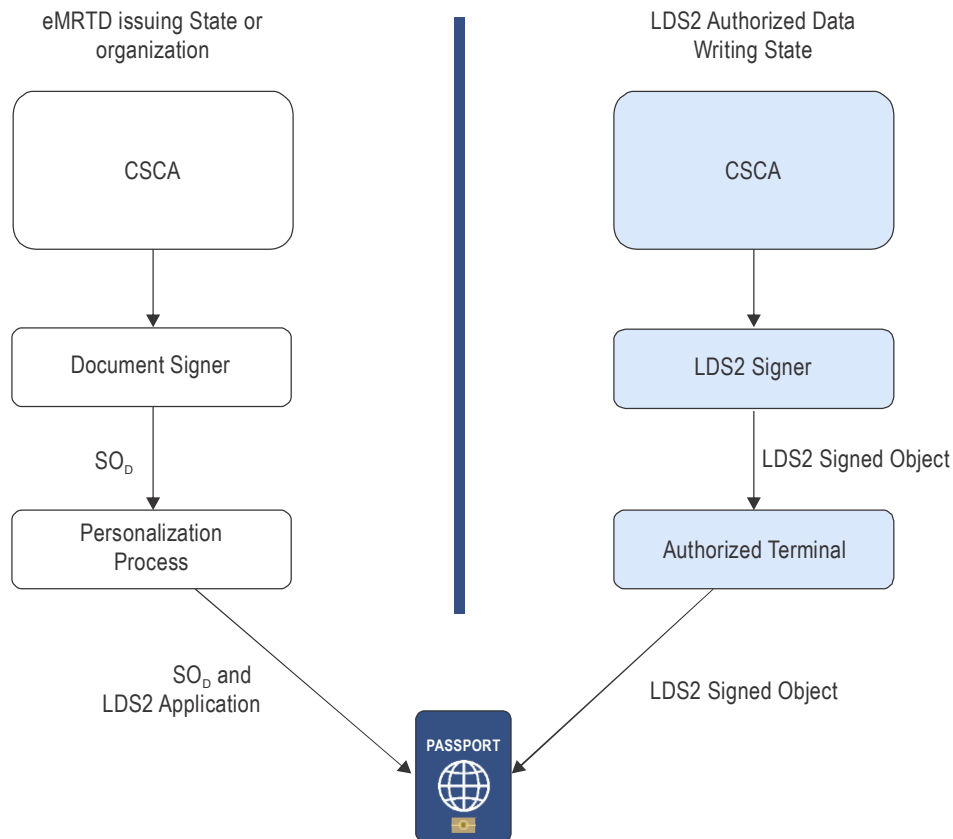


Figure 1. LDS2 Trust Model and Writing Architecture

3.2.1 Country Verifying Certificate Authority

Each issuing State or organization that allows LDS2 data to be added to its eMRTDs MUST set up a single Country Verifying Certificate Authority (CVCA). This CVCA is a Certification Authority (CA) that is the trust anchor for the authorization PKI of that State or organization and covers all LDS2 applications. The CVCA may be a stand-alone entity or it may be integrated with the CSCA of that same State or organization. However, even if co-located, the CVCA MUST use a different key pair than that of the CSCA. The CVCA determines the access rights that will be granted to all Document Verifiers (DV), foreign and domestic, and issues certificates containing the individual authorizations to each of those DVs.

3.2.2 Document Verifier

A Document Verifier (DV) is a CA that, as part of an organizational unit, manages a group of terminals (e.g. terminals operated by a State's border police) and issues authorization certificates to those terminals. A DV MUST have already received an authorization certificate from the responsible CVCA before it can issue associated certificates to its terminals. Certificates issued by a DV to terminals MAY contain the same authorization, or a subset, that has been granted to the DV. They MUST NOT contain any authorization beyond that granted to the DV.

3.2.3 Terminal/Inspection System

Within the context of the authorization PKI, a terminal is the entity that accesses the contactless IC of an eMRTD and writes a digitally signed LDS2 data object, or reads an LDS2 data object. The terminal **MUST** have an authorization certificate issued to it, from its local DV that grants the required authorization. The terminal is also referred to as an Inspection System.

3.2.4 Single Point of Contact (SPOC)

Each State that participates in the LDS2 authorization PKI **MUST** set up a single SPOC. This SPOC is the interface that is used for all communication between the CVCA of one State with the DVs in another State. Certificate requests and responses are communicated between the SPOCs of each State using the SPOC protocol defined in Section 8.

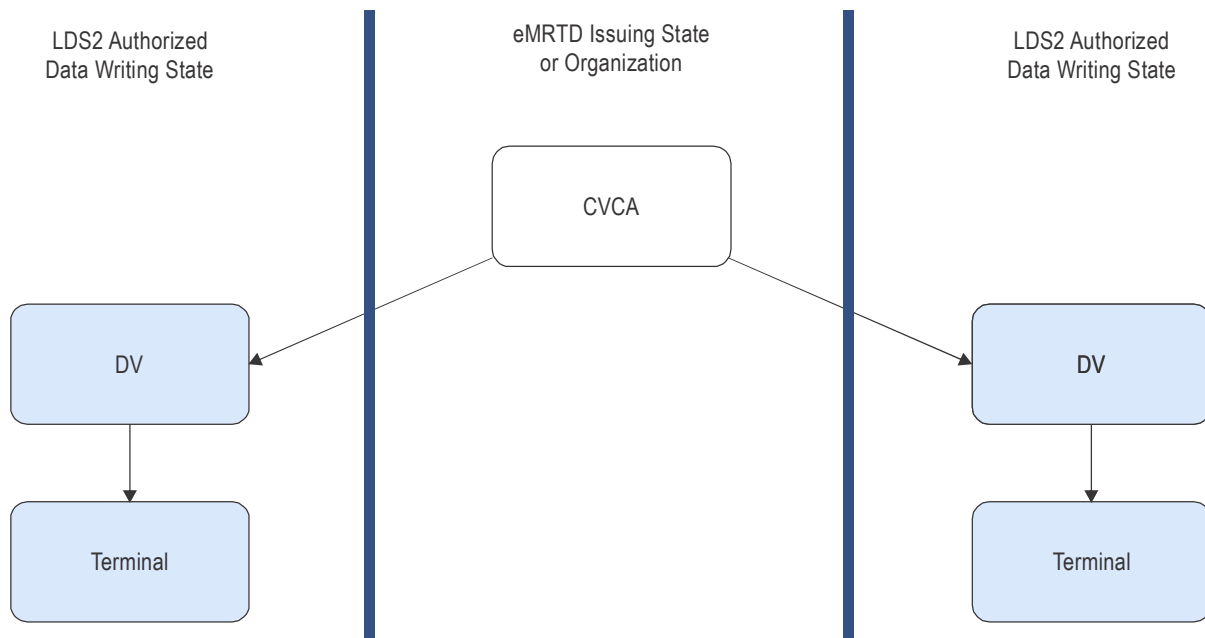


Figure 2. Authorization PKI Trust Model

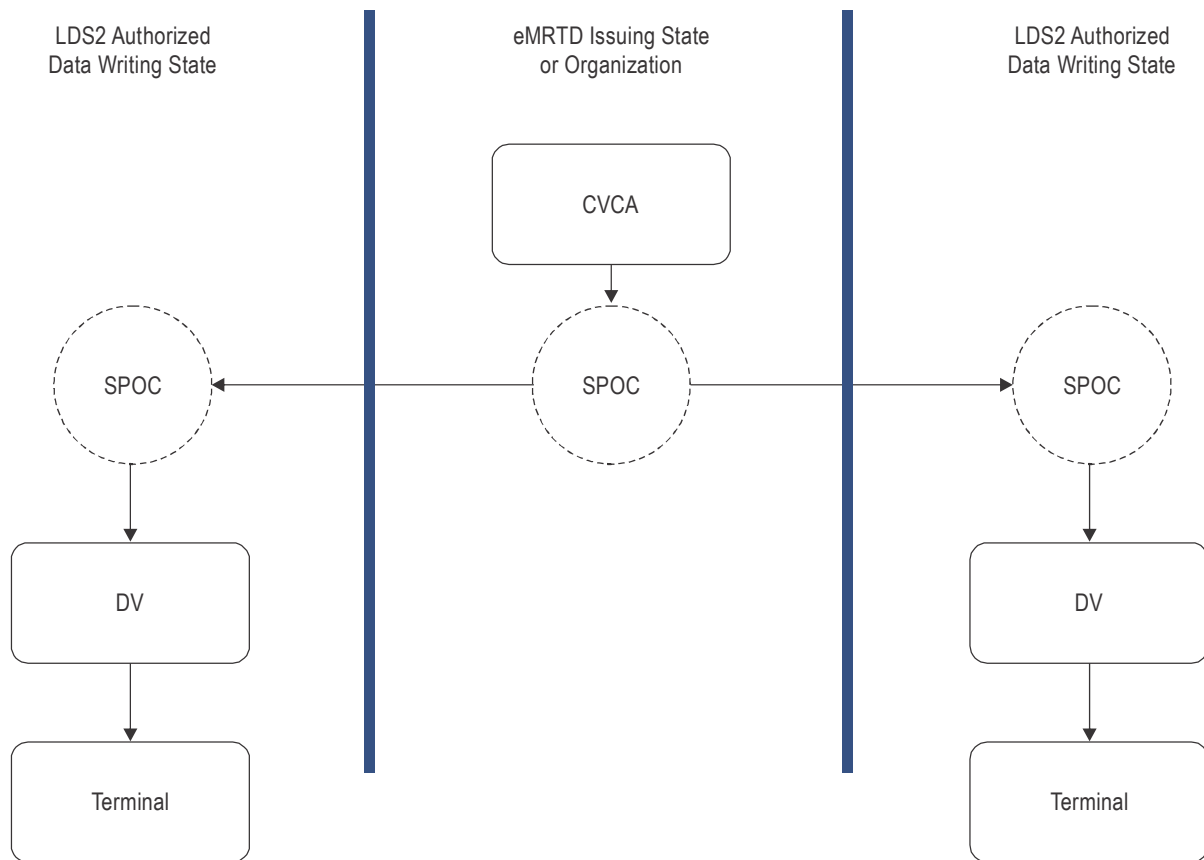


Figure 3. SPOC Role

4. KEY MANAGEMENT

Key Management is defined for the two Public Key Infrastructures separately.

4.1 eMRTD PKI

Issuing States or organizations SHALL have at least two key pair types:

- Country Signing CA key pair; and
- Document Signer key pair.

Issuing States or organizations MAY have additional key pair types:

- Master List Signer key pair;
- Deviation List Signer key pair;
- LDS2 Signer key pair;

- SPOC client key pair;
- SPOC server key pair; and
- Visa Signer key pair/Emergency Travel Document Signer key pair (both are types of Bar Code Signers).

The Country Signing CA, Signer Certificate and SPOC certificate public keys are issued using [X.509] certificates. The public keys contained in CSCA certificates are used to verify the CSCA signature on issued Signer Certificates, SPOC Certificates, CSCA and on issued CRLs.

For Master List Signer, Deviation List Signer and Communications keys and certificates, the private key lifetime and the certificate validity period are left to the discretion of the issuing State or organization.

Both the CSCA certificates and Document Signer certificates are associated with a private key usage and a public key validity period as outlined in Table 1.

Table 1. Key Usage and Validity

	<i>Use of Private Key</i>	<i>Public Key Validity (assuming 10-year valid passports)</i>
Country Signing CA	3-5 years	13-15 years
Document Signer	Up to 3 months ¹	approx. 10 years
LDS2-TS Signer	1-2 years	10 years + 3 months
LDS2-V Signer	1-2 years	10 years + 3 months
LDS2-B Signer	1-2 years	10 years + 3 months
SPOC Client	Not Specified	6-18 months
SPOC Server	Not Specified	6-18 months
Visa Bar Code Signer	1-2 years	Private Key Usage Time + Validity of Visa
Emergency Travel Document Bar Code Signer	1 year + 2 months (the 2 months are meant for smooth roll-over)	Private Key Usage Time + ETD validity timeframe
Master List Signer	Discretion of issuing State or organization	Discretion of issuing State or organization
Deviation List Signer	Discretion of issuing State or organization	Discretion of issuing State or organization
Communication	Discretion of issuing State or organization	Discretion of issuing State or organization

1. Note the corresponding `privateKeyUsage` extension in DS certificate might be slightly longer to allow for overlap or production requirements.

4.1.1 Document Signer Keys and Certificates

The usage period of a Document Signer private key is much shorter than the validity period of the DS certificate for the corresponding public key.

4.1.1.1 Document Signer Public Key validity

The lifetime, i.e. the certificate validity period, of the Document Signer public key is determined by concatenating the following two periods:

- the length of time the corresponding private key will be used to issue eMRTDs, with;
- the longest validity period of any eMRTD issued under that key².

The Document Signer certificate (C_{DS}) SHALL be valid for this total period to enable the authenticity of eMRTDs to be verified. However the corresponding private key SHOULD only be used to issue documents for a limited period; once the last document it was used to issue has expired, the public key is no longer required.

4.1.1.2 Document Signer Private Key issuing period

When deploying their systems, issuing States or organizations may wish to take into account the number of documents that will be signed by any one individual Document Signer private key.

An issuing State or organization may deploy one or more Document Signers, each with its own unique key pair, that are active at any given time.

In order to minimize business continuity costs in the event of a Document Signer certificate being revoked, an issuing State or organization that issues a large number of eMRTDs per day may wish to:

- use a very short private key usage period; and/or
- deploy several concurrent Document Signers that are active at the same time, each with its own unique private key and public key certificate.

An issuing State or organization that issues a small number of eMRTDs per day may choose to deploy a single Document Signer and may also be comfortable with a slightly longer private key usage period.

Regardless of the number of eMRTDs issued per day, or number of Document Signers active at the same time, it is RECOMMENDED that the maximum period any Document Signer private key is used to sign eMRTDs be three months.

Once the last document signed with a given private key has been produced, it is RECOMMENDED that issuing States or organizations erase the private key in an auditable and accountable manner.

2. Some issuing States or organizations may issue eMRTDs before they become valid, for instance on a change of name upon marriage. In these situations, the "longest validity period of any eMRTD" includes the actual validity of the eMRTD (e.g. 10 years) plus the maximum time between when the eMRTD is issued and the time it becomes valid.

4.1.2 LDS2 Signer Keys and Certificates

LDS2 Signer key pairs are similar to Document Signer key pairs in that the usage period of the private key is much shorter than the validity period of the corresponding certificate. The certificates **MUST** remain valid for the lifetime of the eMRTD or the signed LDS2 object (whichever is longest). Because signed data objects will be written to eMRTDs from various States, these certificates **MUST** be valid for at least the duration of the longest eMRTD lifetime (i.e. 10 years).

4.1.2.1 LDS2 Signer Public Key Validity

The lifetime, i.e. the certificate validity period, of the LDS2 Signer public key is determined by concatenating the following two periods:

- The length of time the corresponding private key will be used to sign LDS2 objects, with;
- The validity period of whichever of the following is longest:
 - Any eMRTD that will store an LDS2 object signed with that key; or
 - Any LDS2 object signed with that key. Note that in the case of LDS2 eVisa, it is possible for the validity period of a signed eVisa to extend beyond the validity period of the eMRTD including that visa.

4.1.3 Bar Code Signer Keys and Certificates

A Bar Code Signer is a specific type of signature server used to sign a unique Document Type Category, e.g. a visa, Emergency Travel Document, etc. To follow the best practices in the field, it is **RECOMMENDED** that only a limited number of signing keys (a lower one-digit number) is used in parallel to create signatures for digital seals, unless operational requirements make a larger number of keys absolutely necessary. To ensure availability of the Bar Code Signer in case of a security incident related to the signing keys, it is **RECOMMENDED** to have measures in place to ensure business continuity (e.g. preparation of backup keys, backup site, etc.).

In order to facilitate the handling of the corresponding certificates (see Section 5), the number of published signature validation keys **MUST** be limited to five signature keys per year.

4.1.3.1 Bar Code Signer Public Key Validity

This section applies to all Bar Code Signers, including Visa Signer and Emergency Travel Document Signer.

The lifetime, i.e. the certificate validity period, of the Bar Code Signer public key is determined by concatenating the following two periods:

- the length of time the corresponding private key will be used to issue a Visa or ETD, with;
- the longest validity period of any document issued under that key³.

3. Some issuing States or organizations may issue eMRTDs before they become valid, for instance on a change of name upon marriage. In these situations, the "longest validity period of any eMRTD" includes the actual validity of the eMRTD (e.g. 10 years) plus the maximum time between when the eMRTD is issued and the time it becomes valid.

The Bar Code Signer certificate SHALL be valid for this total period to enable the authenticity of document to be verified. However, the corresponding private key SHOULD only be used to issue documents for a limited period; once the last document it was used to issue has expired, the public key is no longer required.

Private Key Usage Time:	As per document profile
Certificate Validity:	Private Key Usage Time + document Validity Timeframe

Example

Note.— The actual validity periods used for the calculation in this example do not imply any recommendations.

Suppose that documents with a validity period of 5 years are issued, and the private key usage time of the BarCode Signer Certificate is 1 year. Then, the validity of the Bar Code Signer Certificate is $1 + 5 = 6$ years. If the usage time of the private key of the CSCA Certificate is 3 years, then the validity of the CSCA Certificate is $3 + 6 = 9$ years.

4.1.4 CSCA Keys and Certificates

The usage period of a CSCA private key is much shorter than the validity period of the CSCA certificate for the corresponding public key.

4.1.4.1 Country Signing CA Public Key validity

The lifetime, i.e. the certificate validity, of the CSCA public key is determined by concatenating the following periods:

- the length of time the corresponding CSCA private key will be used to sign any certificate below the CSCA; and,
- the maximum key lifetime of any certificate issued below the CSCA.

4.1.4.2 Country Signing CA Private Key issuing period

The usage period for the CSCA private key to sign certificates and CRLs is a delicate balance among the following factors:

- In the unlikely event of an issuing State or organization Country Signing Private CA Key being compromised, then the validity of all eMRTDs issued using Document Signer Keys whose certificates were signed by the compromised CSCA private key is called into doubt. Consequently issuing States or organizations MAY wish to keep the issuing period quite short;
- Keeping the issuing period very short, however, leads to having a very large number of CSCA public keys valid at any one time. This can lead to more complex certificate management within the border processing systems.

It is therefore RECOMMENDED that an issuing State or organization's CSCA key pair be replaced every three to five years.

4.1.4.3 Country Signing CA Re-key

CSCA keys provide the trust points in the whole system and without these the system would collapse. Therefore issuing States or organizations SHOULD plan the replacement of their CSCA key pair carefully. Once the issuance period for the initial CSCA private signing key has elapsed, an issuing State or organization will always have at least two CSCA certificates (C_{CSCA}) valid at any one time.

Issuing States or organizations MUST notify receiving States that a CSCA key rollover is planned. This notification MUST be provided 90 days in advance of the key rollover. Once the key rollover has occurred the new CSCA certificate (certifying the new CSCA public key) is distributed to receiving States.

If the CSCA certificate is a new self-signed certificate, authentication of that certificate should be done using an out-of-band method.

When a CSCA key rollover occurs a certificate MUST be issued that links the new key to the old key to provide a secure transition for relying parties. Generally this is achieved through the issuance of a self-issued-certificate where the issuer and subject fields are identical but the key used to verify the signature represents the old key pair and the certified public key represents the new key pair. These CSCA Link certificates need not be verified using an out-of-band method as the signature on the CSCA Link certificate is verified using an already trusted public key for that CSCA. Master Lists can also be used to distribute CSCA Link and CSCA self-signed root certificates.

Issuing States or organizations should refrain from using their new CSCA private key for the first two days after the CSCA key rollover, to ensure the corresponding new CSCA public key certificate has been distributed successfully.

Issuing States or organizations MUST use the newest CSCA private key for signing all certificates, and for signing CRLs.

4.1.5 Certificate Revocation

Issuing States or organizations may need to revoke certificates in case of an incident (like a key compromise).

All CSCAs MUST produce periodic revocation information in the form of a Certificate Revocation List (CRL).

CSCAs MUST issue at least one CRL every 90 days, even if no certificates have been revoked since the previous CRL was issued. CRLs MAY be issued more frequently than every 90 days but not more frequently than every 48 hours.

If a certificate is revoked, a CRL indicating that revocation MUST be distributed within 48 hours.

Only certificates can be revoked, not Document Security Objects. The use of CRLs is limited to notifications of revoked certificates that had been issued by the CSCA that issued the CRL (including revocation notices for CSCA certificates, DS certificates, Master List Signer certificates, Deviation List Signer certificates and any other certificate types issued by that CA).

Partitioned CRLs are not used in the eMRTD application. All certificates revoked by a CSCA, including DS certificates, CSCA certificates, Master List Signer certificates and Deviation List Signer certificates are listed on the same CRL. Although the CRL is always signed with the newest (current) CSCA private signing key, the CRL includes revocation notices for certificates signed with that same private key as well as certificates signed with earlier CSCA private signing keys.

4.1.5.1 Revocation of CSCA Certificates

Revocation of a CSCA certificate is both extreme and difficult. Upon informing a receiving State that a CSCA certificate has been revoked, all other certificates signed using the corresponding CSCA private key are effectively revoked.

Where a CSCA Link certificate has been signed using an old CSCA private key to certify a new CSCA public key (see “Country Signing CA Re-key” in 4.1.4.3), revoking the old CSCA certificate SHALL also revoke the new CSCA certificate.

If a CSCA certificate needs to be revoked, the CSCA may issue a CRL signed with the private key that corresponds to the public key being revoked, as this is the only key users of the CRL will be able to verify at that time. The CSCA public key should be considered valid only for the purpose of verifying that CRL signature. Once a CRL user has verified the CRL signature, the CSCA private signing key is considered compromised and the certificate revoked for all future verifications.

To issue new documents, the issuing State or organization MUST revert to bootstrapping its authentication process from the beginning, by issuing a new CSCA Root certificate, distributing that certificate to receiving States, and supporting out-of-band confirmation that the certificate received by each receiving State is in fact the current authentic CSCA certificate.

4.1.5.2 Revocation of other Certificates

When an issuing State or organization wishes to revoke a Signer certificate issued under the CSCA, it does not need to wait until the `nextUpdate` period in the current CRL is due to issue a new CRL. It is RECOMMENDED that a new CRL be issued within a 48-hour period of revocation notification.

4.1.6 Cryptographic Algorithms

An issuing State or organization MAY support different algorithm for use in their CSCA and Signing Certificate keys. For example, the CSCA may have been issued using RSA, but Signer Certificates could be Elliptic Curve DSA (ECDSA) and vice versa.

Issuing States or organizations SHALL choose appropriate key lengths offering protection against attacks. Suitable cryptographic catalogues SHOULD be taken into account.

Receiving States MUST support all algorithms at points where they wish to validate the signature on eMRTDs.

For use in their CSCA, Signing keys and, where applicable, Document Security Objects, issuing States or organizations SHALL support one of the algorithms below.

4.1.6.1 RSA

Those issuing States or organizations implementing the RSA algorithm for signature generation and verification of certificates and the Document Security Object (SO_D) SHALL use [RFC 4055]. [RFC 4055] specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. It is RECOMMENDED that issuing States or organizations generate signatures according to RSASSA-PSS, but receiving States MUST also be prepared to verify signatures according to RSASSA-PKCS1_v15.

4.1.6.2 Digital Signature Algorithm (DSA)

Those issuing States or organizations implementing DSA for signature generation or verification SHALL use [FIPS 186-4].

4.1.6.3 Elliptic Curve DSA (ECDSA)

Those issuing States or organizations implementing ECDSA for signature generation or verification SHALL use [X9.62] or [ISO/IEC 15946]. The elliptic curve domain parameters used to generate the ECDSA key pair MUST be described explicitly in the parameters of the public key, i.e. parameters MUST be of type ECPParameters (no named curves, no implicit parameters) and MUST include the optional co-factor. ECPoints MUST be in uncompressed format.

It is RECOMMENDED that the guideline [TR 03111] be followed.

4.1.6.4 Hashing Algorithms

SHA-224, SHA-256, SHA-384 and SHA-512, are the only permitted hashing algorithms. See [FIPS 180-2].

4.1.7 Cryptographic Algorithms for LDS2 Signer Certificates

Because LDS2 certificates and signed objects are stored on the contactless IC, they need to be as compact as possible. Therefore LDS2 Signers MUST use ECDSA, irrespective of the algorithm used in the CSCA and Document Signing keys.

4.2 Authorization PKI

Issuing States or organizations that implement LDS2 SHALL have the following key pair types:

- Country Verifying CA (CVCA) Key Pair;
- Document Verifier (DV) Key Pair; and
- Terminal Key Pair.

The CVCA and DV public keys are certified by the CVCA. The terminal public keys are certified by the DV. CVCA, DV and terminal public key certificates are card-verifiable certificates that MUST comply with their respective certificate profiles defined in Section 7. There is no revocation mechanism for CVCA, DV or terminal certificates. Therefore their validity periods are much shorter than the X.509 certificate types.

The private key usage period is not specified and is up to the discretion of the State. However, the private key usage period MUST be at most equal to the public key validity period. The public key validity period for CVCA, DV and terminal key pairs is outlined in Table 2.

Table 2. Key Usage Card-Verifiable Certificate Validity

	Public Key Validity
CVCA	6 months – 3 years
DV	2 weeks – 3 months
Terminal	1 day – 1 month

4.2.1 Cryptographic Algorithms for Terminal Authentication

The algorithm used for Terminal Authentication in the authorization PKI is determined by the CVCA of the eMRTD issuing State. The same signature algorithm, domain parameters and key sizes **MUST** be used within a certificate chain (i.e. the CVCA, DV and terminal certificates for a given authorization). As a consequence, Document Verifiers and terminals will have to be provided with several key pairs. CVCA Link Certificates **MAY** include a public key that deviates from the current parameters, i.e. the CVCA **MAY** switch to a new signature algorithm, new domain parameters, or key sizes.

For Terminal Authentication, either RSA or ECDSA **MAY** be used. Details are provided in Doc 9303-11.

4.2.2 Cryptographic Algorithms for SPOC

The TLS Encryption Suites to be used for the SPOC protocol are listed in Table 3.

Table 3. TLS Encryption Suites

Cipher Suite	Certificate and Key Exchange Algorithm
TLS_RSA_WITH_AES_128_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE_ECDSA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA

In the scope of the TLS handshake negotiation, the client **SHALL** support all the TLS cipher suites defined in Table 3. Both the server and the client side **SHALL** support RSA and ECDSA-based authentication. It is permissible for a server to request and also for the client to send a client certificate of a different type than the server certificate.

The use of the ECDHE_ECDSA key agreement in TLS handshake is in accordance with the additions defined in [TLSECC], [TLS1.2] and [TLSEXT]. Both the client and the server SHALL support the appropriate elliptic curves extensions as specified in [TLSECC] specification in the scope of TLS handshake. The supported elliptic curves and EC Point formats are defined in Section 5 of [TLSECC]. The use of the supported TLS cipher suites defined in Table 3 which uses Advanced Encryption Standard (AES) for encryption SHALL be in accordance with [TLSAES] specification.

5. DISTRIBUTION MECHANISMS

For eMRTD PKI, the PKI objects need to be distributed to the receiving States. A number of different distribution mechanisms are used, depending on the type of object and operational requirements. It is important to note that distribution of these objects does NOT establish trust in those objects, or the private/public keys associated with them. Mechanisms for establishing trust are specified in Section 6.1.

The distribution mechanism for the Authorization PKI is covered in Section 8.

The objects that need to be distributed from issuing States or organizations to receiving States include:

- CSCA certificates;
- CSCA Link Certificates;
- Document Signer certificates;
- LDS2 Signer certificates;
- Initial CVCA certificates;
- CVCA Link certificates;
- DV certificates;
- Bar Code Signer certificates;
- CRLs (null and non-null);
- Master List Signer certificates; Master Lists; and
- Deviation List Signer certificates; Deviation Lists.

The distribution mechanisms used in the eMRTD and Authorization PKI include:

- PKD;
- Bilateral exchange;
- SPOC;
- Master Lists;

- Deviation Lists; and
- eMRTD contactless IC.

A primary and secondary (where relevant) distribution mechanism is specified for each object as outlined in Table 4.

Table 4. Distribution of PKI Objects

	Contactless IC	SPOC	Bilateral	PKD	Deviation List	Master List	Notes
CSCA Certificates			Y (primary)			Y (secondary)	
Document Signer Certificates	Y (primary)			Y (secondary)			Certificates written at same time SOD is written
LDS2 Signer certificates	Y						Certificates written at same time signed object is written
CVCA Initial Certificate	Y						Certificate written at eMRTD personalization time
CVCA Link Certificates	Y	Y					Certificates distributed to DVs via SPOC and CVCA Trust Anchor updated on contactless IC at next verification
DV Certificates		Y					Distributed only to subject DV
CRLs (Null and Non-null)			Y (secondary)	Y (primary)			CRLs issued by CSCA include revocation information relevant to LDS2 PKI objects
Master List Signer Certificates						Y	
Bar Code Signer Certificates			Y (secondary)	Y (primary)			Bar Code Signers are not encoded in the Bar Code and hence distribution must be ensured for validation of bar code
Master Lists			Y	Y			
Deviation List Signer Certificates					Y		

Operationally, receiving States are not obliged to use both the primary and secondary source. In the daily operation of an Inspection System, it is at the inspecting authority's discretion whether to use the primary or the secondary source. If the authority of the receiving State uses the secondary source for a certificate or CRL in its daily operations, it should be prepared to support the primary source as well.

Issuing States or organizations need to plan their key pair rollover strategies for both CSCA keys and Signer Keys in order to enable propagation of certificates and CRLs into receiving States' border control systems in a timely manner. Ideally propagation will occur within 48 hours, but some receiving States may have remote and poorly connected border outposts to which it may take more time for certificates and CRLs to propagate out. Receiving States SHOULD make every effort to distribute these certificates and CRLs to all border stations within 48 hours.

Issuing States or organizations should expect that CSCA certificates (C_{CSCA}) will be propagated by receiving States within 48 hours.

Issuing States or organizations ensure the timely propagation of Document Signer certificates (C_{DS}) by including the Document Signer certificate (C_{DS}) within the Document Security Object (SO_D). They should expect that Document Signer certificates (C_{DS}) published in the PKD will also be propagated to border stations within 48 hours.

The Bar Code Signer Certificates are not contained in the digital seal itself. Hence, a country that issues documents protected with digital seals MUST publish all its Bar Code Signer Certificates. The primary distribution channel for Bar Code Signer Certificates is PKD/bilateral. Other mechanisms, e.g. publication on a website, are secondary channels.

For Bar Code Signers, Publication MUST adhere to the following principles:

- as soon as a new certificate is created, it MUST be published with a delay of no more than 48 hours; and
- the certificates MUST remain published until their expiration or revocation.

Receiving States SHOULD make every attempt whether electronically or by other means to act upon CRLs, including those CRLs issued under exceptional circumstances.

Timely propagation of Master List Signer certificates is ensured by including them within each Master List.

5.1 PKD Distribution Mechanism

ICAO provides a Public Key Directory (PKD) service. This service SHALL accept PKI objects, including certificates, CRLs and Master Lists, from PKD participants, store them in a directory, and make them accessible to all receiving States.

CSCA certificates (C_{CSCA}) are not stored individually as part of the ICAO PKD service. However, they may be present in the PKD if they are contained on Master Lists.

Every certificate remains in the PKD until its certificate validity period has expired, regardless of whether or not the corresponding private key is still in use.

Certificates, CRLs and Master Lists stored in the PKD by all PKD participants SHALL be made available to all parties (including non-PKD participants) that need this information for validating the authenticity and integrity of digitally stored eMRTD data, LDS2 Objects and VDS objects.

5.1.1 PKD Upload

Only PKD participants MAY upload certificates, CRLs and Master Lists to the PKD. All certificates and CRLs MUST comply with the profiles in Section 7. All Master Lists MUST comply with the specifications in Section 9.

The PKD consists of a “Write Directory” and a “Read Directory”. PKD participants SHALL use the Lightweight Directory Access Protocol (LDAP) to upload their objects to the Write Directory. Once the digital signature has been verified on an object, and other due diligence checks completed, the object is published in the Read Directory.

5.1.2 PKD Download

Read access to all certificates, CRLs and Master Lists published in the PKD SHALL be available to PKD participants and non-participants. Access control SHALL NOT be implemented for PKD read access.

It is the receiving State’s responsibility to distribute objects downloaded from the PKD to its Inspection Systems and to maintain a current CRL cache along with the certificates necessary to verify the signatures on eMRTD data.

5.2 Bilateral Exchange Distribution Mechanism

For CRLs and CSCA certificates (C_{CSCA}), the primary distribution channel is bilateral exchange between issuing States or organizations and receiving States. Bilateral exchange can also be used to distribute Master Lists.

The specific technology used for that bilateral exchange may vary depending on the policies of each issuing State or organization that has a need to distribute its certificates, CRLs and Master Lists, as well as the policies of each receiving State that needs access to those objects. Some examples of technologies that may be used in bilateral exchange include:

- diplomatic courier/pouch;
- email exchange;
- download from a website associated with the issuing CSCA; and
- download from an LDAP server associated with the issuing CSCA.

This is not an exhaustive list and other technologies may also be used.

5.3 Master List Distribution Mechanism

Master Lists are a supporting technology for the bilateral distribution scheme. As such, distribution of CSCA certificates via Master Lists is a subset of the bilateral distribution scheme.

A Master List is a digitally signed list of the CSCA certificates that are “trusted” by the receiving State or organization 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 or organizations 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.

A Master List Signer is authorized by a CSCA to compile, digitally sign, and issue Master Lists. Master Lists **MUST NOT** be signed and issued directly by a CSCA itself. Master List Signer certificates **MUST** comply with the certificate profile defined in Section 7.

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.

Each Master List **MUST** include the Master List Signer's certificate that will be used to verify the signature on that Master List as well as the CSCA certificates of the CSCA that issued that Master List Signer certificate.

If new CSCA certificates have been received by a receiving State, and its validation procedures have been completed, it is **RECOMMENDED** that a new Master List be compiled and issued.

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 (see Section 6 for details).

6. PKI TRUST AND VALIDATION

PKI Trust and Validation differ between the eMRTD PKI and Authorization PKI.

6.1 eMRTD PKI

In the eMRTD PKI environment, the Inspection Systems in receiving States act in the role of PKI relying parties. Successful verification of the digital signature on the Document Security Object of an eMRTD ensures the authenticity and integrity of the data stored on the contactless IC of that eMRTD. That signature verification process requires that the relying party establish that the Document Signer public key used to verify the signature is itself "trusted".

The various distribution mechanisms defined in Section 5 allow receiving States to gain access to the certificates and CRLs that they need to verify digital signatures in question. However, these distribution schemes do not establish trust in those certificates, CRLs or the public keys that will be used to verify signatures on those certificates and CRLs.

The public keys contained in CSCA certificates (CCSCA) are used to verify the digital signature on certificates and CRLs. Therefore, to accept an eMRTD from another issuing State, the receiving State **MUST** already have placed into some form of trust store, accessible by their border control system, a trusted copy of the issuing State or organization CSCA certificate (CCSCA), or other form of Trust Anchor information for that CSCA public key as derived from the certificate.

It is a receiving State's responsibility to establish trust in the CSCA certificates (CCSCA) and store the certificates (or information from the certificates) as Trust Anchors, in a secure way for use by their border inspection systems.

6.1.1 Trust Anchor Management

As specified in [RFC 5280] a Trust Anchor must be established that can be used to anchor the validation procedure for a given Document Signer, Master List Signer, Deviation List Signer or other type of certificate.