International Civil Aviation Authority (ICAO)

Master List Policy and Procedure

Version 1.0

Table of Contents

International Civil Aviation Authority (ICAO) 1

Master List Policy and Procedure 1

1. Introduction 3

2. Background 4

2.1 ICAO Public Key Directory (ICAO PKD): Status as of 2019 with respect to CSCA masterlists 4

2.2 New Developments in 2020 4

3. ICAO Master List Creation 5

3.1 CSCA Source 5

3.2 CSCAs for the Master List - Selection 5

3.3 Master List Creation and Signing 5

4. ICAO Master List Distribution 6

5. Master List and Certificate Revocation List (CRL) 7

5.1 ICAO Master List CRL Policy 7

6. CSCA Master List Signing Certificate 8

6.1 Certificate Profile 8

Glossary

CA	Certificate Authority
CSCA	Country Signing Certificate Authority
DSC	Document Signer Certificate
CRL	Certificate Revocation List
ML	Master List
MLS	Master List Signer
DL	Deviation List
DLS	Deviation List Signer
EMA	eMRTD Authority
eMRTD	Electronic Machine Readable Travel Document
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
LDAP	Lightweight Directory Access Protocol
NPKD	National Public Key Directory, a nationally-implemented solution that enables appropriate storage and/or dissemination of digital certificates and other data necessary for authentication of eMRTDs, often connected to the ICAO PKD and storing the information obtained therein a local representation of the ICAO PKD
PKD	Public Key Directory, used to store and distribute DSCs, CRLs, Master Lists and/or Deviation Lists
PKI	Public Key Infrastructure
SOD	Document Security Object
UN	United Nations
ICAO ML	The ICAO Master List, this is the Master List of CSCA certificates created by ICAO and signed using the ICAO Master List Signer.

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's 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).

Doc 9303 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 Doc 9303 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 International Civil Aviation Authority (ICAO) Master List (ML) Policy and Procedures document sets out the conditions and policy for the creation of a ML that will be signed by the ICAO Master List Signer (MLS) and made available publically.

2. Background

2.1 ICAO Public Key Directory (ICAO PKD): Status as of 2019 with respect to CSCA masterlists

The ICAO PKD consists of a directory with a Lightweight Directory Access Protocol (LDAP) structure that is accessed (for upload and/or download) through an LDAP interface using either certificate-based access credentials or password-based access credentials. The contents of the PKD are also available for public download through the dedicated website made available for such; public download is subject to the terms and conditions delineated therein, principally that the data should not be used for commercial purposes.

The ICAO PKD supports management of all certificate types currently in use for eMRTDs, albeit that hitherto only ICAO PKD Participants' DSCs, Certificate Revocation Lists (CRLs), MLs, and Deviation Lists (DLs) are available for download.

Every active ICAO PKD member has a CSCA certificate in the ICAO PKD. Initially, the CSCA certificate is provided to ICAO through bilateral exchange, following strictly defined procedures. Subsequent updates to the CSCA certificate may be transmitted bilaterally or using Link Certificates.

Up to now, the CSCA certificates stored by the ICAO PKD HSM are ONLY used to verify DSCs, CRLs, MLSs and DLSs uploaded by the ICAO PKD Participant that is associated with the corresponding CSCA. The ICAO PKD does not distribute these CSCA certificates as a part of normal ICAO PKD operations. As the CSCA certificates are securely stored in an HSM, they are not a part of the accessible LDAP structure that is used to store other certificates.

2.2 New Developments in 2020

From 2020 onwards, ICAO will prepare its own ML of CSCA certificates to be made available to interested parties through the ICAO PKD according to the applicable rules already established for use of data in the ICAO PKD (in particular, we refer to the ICAO PKD Regulations and Procedures document available on the PKD public website as well as the afore-mentioned rules for public download available on the download website). Use of the CSCA certificates thus made available is intended to improve States' capabilities to verify the authenticity and integrity of eMRTDs presented as well as to facilitate the easy provision of relevant PKI data related to a state's eMRTDs to the authorized users and recipients of ICAO PKD data as per Section 4 of this document.

3. ICAO Master List Creation

3.1 CSCA Source

All CSCA certificates that are to be included in the ICAO ML MUST be received from PKD participants via bilateral exchange or verified based on a certificate chain in which the root certificate was thus obtained (i.e. using link certificates).

3.2 CSCAs for the Master List - Selection

a. Only certificates stored in the ICAO PKD HSM may be included in the ICAO ML.

b. Any certificate that is rejected by ICAO prior to such upload MUST NOT be included in the ICAO ML.

Procedures outlined in the 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."

3.3 Master List Creation and Signing

CSCAs and their corresponding Link Certificates, where available to ICAO, and taken from the ICAO PKD HSM, may be included in the ICAO ML.

An ML Signer certificate will be issued by the UN on foot of a request from ICAO. The signed certificate, prepared following secure exchange of the request and certificate between ICAO and the UN using ICAO and/or UN IT data exchange platforms only, will be imported into the ICAO PKD HSM for signing of the ML. All technical procedures for the creation and import of the ICAO ML Signer certificate are detailed in Chapter 8 of the ICAO PKD - Operator Manual.

Technical procedures for the creation of the ICAO ML are detailed in Chapter 8.4 of the ICAO PKD - Operator Manual.

New MLs will be issued at approximately 3-monthly intervals when appropriate (i.e. due to the availability of new CSCA certificates)

4. ICAO Master List Distribution

The ICAO ML may be distributed using the following methods:

- Hand Delivered by an ICAO Officer
- Email from an @icao.int account
- Using the public download site at https://download.pkd.icao.int/, subject to the terms and conditions for such download laid out therein
- Through the dedicated website for download of the ICAO ML – https://www.icao.int/Security/FAL/PKD/Pages/ICAO-Master-List.aspx - subject to the terms and conditions laid out therein
- Through the ICAO PKD

All ICAO MLs **will** be uploaded to the ICAO PKD into the UN LDAP Directory, by the UN.

Procedures for the ICAO PKD upload process are described in the UN PKI Documentation relating to ICAO PKD uploads.

When distributing the ICAO ML the following extract from Doc 9303 will be clearly presented, alongside the relevant provisions of Section 7 of the <<COOPERATION AGREEMENT BETWEEN THE UNITED NATIONS AND THE INTERNATIONAL CIVIL AVIATION ORGANIZATION FOR THE DIGITAL SIGNING OF ICAO MASTER LIST.>>

"*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 ICAO ML, ICAO provides a service. It does not assert that the certificates contained within the ICAO ML are trusted, only that due diligence has been performed by ICAO in the creation of the ICAO 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 ICAO to ensure that a state that receives the ICAO ML has access to CRLs for all of the States whose CSCAs are contained in the ICAO ML

5.1 ICAO Master List CRL Policy

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

It is up to the State receiving and using the ICAO 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 Master List Signing Certificate

6.1 Certificate Profile

ICAO Doc 9303 Part 12 leaves the Private Key Usage Period for the MLSs to “the discretion of the State”.

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