International Civil Aviation Authority (ICAO)

Health Master List Policy and Procedure

Version 1.0

Table of Contents

Glossary

CA	Certificate Authority
CSCA	Country Signing Certificate Authority
BSC	Barcode Signer Certificate
CRL	Certificate Revocation List
ML	Master List
MLS	Master List Signer
HCSCA	A CA certificate that is a root of trust for health credentials used in travel
HSM	Hardware Security Module
ICAO	International Civil Aviation Organization
ICAO HML	The ICAO Health Master List, this is the Master List of CA certificates associated with issuance of health credentials used in travel created by ICAO and signed using the ICAO Health Master List Signer.
PKI	Public Key Infrastructure
VDS-NC	The ICAO specified Visible Digital Seal for Non-Constrained Environments

1. Introduction

The International Civil Aviation Organization (ICAO) published the Technical Report (TR) "VDS-NC Visible Digital Seal for Non-Constrained Environments"[1] in April 2021. The TR introduced specifications for a 2D barcode – the VDS-NC – with use cases for encoding of secure, machine-readable health proofs (certificates of vaccination and certificates of testing) that could be presented in travel. Publication of the TR was a response to issuance of recommendations by the ICAO Council Aviation Recovery Task Force (CART) that such proofs could be useful in the context of cross-border travel during the COVID-19 pandemic.

The VDS-NC specifications prescribe a trust model that generally follows that already established for electronic Machine Readable Travel Documents (eMRTD), defined in ICAO Doc 9303 Part 12. The VDS-NC barcodes are digitally signed using certificates that are part of a two-layer certificate chain that enables an inspection system to verify the authenticity and integrity of the data stored in the barcode. The TR recommends use of the existing CSCA certificate associated with travel documents as the root of trust, with the CSCA in this context signing a BSC that itself signs the barcode. Notwithstanding, it allows use of a new root of trust that would be specific for health use cases. As a consequence, methods must be made available for the distribution of health certificates associated with VDS-NC that complement those already in place for travel document certificates (namely bilateral exchange and distribution via the ICAO PKD. The TR indicates that the PKD should be a distribution mechanism for both health CAs (hereafter referred to as HCSCAs) and health BSCs. In addition, revocation of certificates is accomplished using CRLs, and the PKD should provide for distribution of health CRLs.

It is noted that the World Health Organization (WHO) set up its own Working Groups that examined the preparation of health proofs, including for use in travel. The Digital Documentation of COVID-19 Certificates (DDCC) Working Group (working under a revised scope to that of the previously-established Smart Vaccination Certificate Working Group) has published technical specifications and implementation guidance[2] for issuance of health proofs. The proofs outlined are digitally-signed records that should generally use a national two-layer PKI-based trust architecture. The VDS-NC is entirely consistent with this guidance. The WHO will not set up its own distribution mechanism for health proofs certificates at this stage, and hence the ICAO initiative will support efforts to implement health proofs that are conformant to the WHO DDCC specifications and guidance.

The PKD should soon be enhanced in order to provide for distribution of health-related certificates. In the interim, a solution is being set up with the support of INCERT Luxembourg in

[1] Available at:

https://www.icao.int/Security/FAL/TRIP/PublishingImages/Pages/Publications/Visible%20Digital%20Seal%20for%20non-constrained%20environments%20%28VDS-NC%29.pdf

[2] Digital Documentation of COVID-19 Certificates: Vaccination Status — Technical Specifications and Implementation Guidance, 27 August 2021. Geneva: World Health Organization; 2021 (WHO/2019-nCoV/Digital_certificates/vaccination/2021.1). Licence CC BY-NC-SA 3.0 IGO.

order to allow for distribution of the most critical certificates associated with health proofs. As the VDS-NC encodes the BSC certificate as part of the barcode itself, only the root certificate (HCSCA or CSCA as appropriate) and associated CRL are required in order to fully validate the integrity and authenticity of the barcode. The solution thus is based around the publication of an ICAO-conformant Master List to distribute HCSCAs alongside the publication of health CRLs on the ICAO website.

As per Doc9303:

> "*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)

This International Civil Aviation Authority (ICAO) Health Master List (HML) Policy and Procedures document sets out the conditions and policy for the creation of a HML that will be signed by a Master List Signer (MLS) established specifically for this purpose and made available publically. It is applicable to the HML prepared in cooperation with INCERT Luxembourg. A new version of this document will be prepared for the future publication of a HML through the ICAO PKD.

2. ICAO Health Master List Creation

2.1 CA Source

All HCSCA certificates that are to be included in the ICAO HML MUST be received from health proof issuing entities via bilateral exchange or verified based on a certificate chain in which the root certificate was thus obtained (i.e. using link certificates to a travel document CSCA or to a known HCSCA). In the case of bilateral exchange, documentary evidence of such handover will be recorded and signed by both parties with an out-of-band validation being performed in accordance with the document "ICAO Public Key Directory (PKD) Key Ceremony Procedures" dated 7 May 2020. If a State uses the travel document CSCA in order to sign health proofs, that CSCA certificate may be included in the HML if the travel document CSCA is already on the ICAO PKD HSM and thus accepted by ICAO in accordance with applicable PKD procedures. Thus, ICAO is complying with the obligations ascribed to issuing authorities in Doc9303:

"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."

2.2 HCSCAs for the Master List - Selection

ICAO will only carry out rudimentary assessment of the HCSCAs obtained in order to assess that they are appropriately signed CA certificates and that they are in binary (.der) format. Full conformance to ICAO specifications will not be assessed. It is not necessary that the HCSCA obtained is used for issuance of VDS-NC based health proofs – any root of trust for health certificates in current use may be included.

Adherence to the responsibilities of the issuing authority with regard to MLs outlined in Doc 9303 is stressed:

"A receiving State making use of Master Lists MUST still determine its own policies for establishing trust in the certificates contained on that list."

2.3 Master List Creation and Signing

HCSCAs and their corresponding Link Certificates, where available to ICAO and validated as per section 2.2, will be included in the ICAO HML.

A new ICAO CA will be established for the purposes of signing the HML, using the two-letter code IA (International Aviation) and the three-letter code IAO (International Aviation Organization). Suitable notification/registration of these codes is being sought by ICAO at the time of writing. An ML Signer certificate will be issued under this CA for signature of the ICAO HML. The ICAO CA private key will be stored in secure, offline infrastructure at all times while the ML Signer private key certificate will be securely stored in a dedicated HSM as described in the Document "An overview of the infrastructure for issuance of the ICAO Health Master List" (confidential).

New HMLs will be issued regularly and when appropriate (i.e. due to the availability of new CA certificates).

3. ICAO Master List Distribution

The ICAO HML may be distributed using the following methods:

- Hand Delivered by an ICAO Officer
- Email from an @icao.int account
- Through the dedicated website for download of the ICAO HML – https://www.icao.int/Security/FAL/PKD/Pages/ICAO-Master-List.aspx (or another URL under the PKD domain) - subject to the terms and conditions laid out therein

When distributing the ICAO HML the following extract from Doc 9303 will be clearly presented.

"*Use of a Master List does enable more efficient distribution of HCSCA 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 HML, ICAO provides a service. It does not assert that the certificates contained within the ICAO HML are trusted, only that due diligence has been performed by ICAO in the creation of the ICAO HML as described in this document.

4. Health 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 HML has access to CRLs for all of the States whose HCSCAs are contained in the ICAO HML. Notwithstanding, ICAO will provide links to all CRL distribution points notified to it (or obtained from the HCSCA certificate and verified to be active) on a dedicated page of the ICAO PKD public website. The CRL associated with the ICAO CA established for signature of the HML will also be made available on the site. The CRL will be re-issued at least every 90 days in accordance with the provisions of Doc 9303.

4.1 ICAO Health Master List CRL Policy

HCSCAs 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 HML.

It is up to the State receiving and using the ICAO HML and its contents to determine its own policy with regards to accepting a HCSCA for which they do not have access to the corresponding CRLs.

5. CSCA Master List Signing Certificate

5.1 Certificate Profile

ICAO Doc 9303 Part 12 provides flexibility in the validity period of CSCA certificates but generally advises that the Private Key Usage Period be approximately 3-5 years. ICAO Doc 9303 Part 12 leaves the Private Key Usage Period for the MLSs to "the discretion of the State".

The ICAO CA established for use in the context of the HML has a Private Key Usage Period of 3 years and a validity period of 3 years and 3 months.

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 12 months.