ICAO Public Key Directory (PKD)

Key Ceremony Procedures

Update for ICAO PKD Service 2020

Table of Contents

1. Introduction

The CSCA is the Country Signing Certificate Authority. Each participant needs to import at least one CSCA certificate as its trust anchor into the ICAO PKD system before uploads of Document Signer Certificates, CRLs, Master Lists or Deviation Lists can be done through the PKD electronic interface.

The process by which a CSCA is imported into the ICAO PKD is known as a key ceremony. These key ceremonies are done at the ICAO HQ in Montreal by the ICAO PKD office.

2. Key ceremony Overview

The key ceremony for CSCA and CSCA Link certificates is a formal procedure to import the CSCA certificates into the ICAO PKD System after checking their conformance to ICAO standards. Key ceremonies are always done in 2 steps:

Step 1: registration of a key ceremony. This is done to make sure that the key ceremony can be carried out successfully (check personal data of the representative of a participant state, check the correctness and conformance of the CSCA certificates)

Step 2: key ceremony with import of the CSCA certificate into the HSM

There are basically two types of key ceremonies:

a) Key ceremony with **self-signed CSCA certificates**:
   These standalone certificates are not linked with a previously imported CSCA and need the presence of an authorized representative of the participating state during the key ceremony. In advance, the CSCAs have to be submitted in a secure manner to prepare the key ceremony and to validate the certificates.

b) Key ceremonies with CSCA certificates and corresponding **CSCA Link certificates**:
   For renewing CSCA certificates participant states should use CSCA Link certificates. These certificates can be provided to the ICAO PKD Office in a secure manner and are then imported by ICAO on behalf of the participant state. This procedure does not require the presence of a representative of the state.

While this document focuses on the production environment, a few words to the pre-production environment. Only self-signed CSCAs are used. To provide a new CSCA, the PKD support is contacted via its PKD online support system (preferred) or via email (pkdsupport@veridos.com) to provide the test CSCA to be imported into the Pre-Production. The PKD support will prepare and initiate the key ceremony in the pre-production environment while updating the participant accordingly.

3. Definition of roles

Role	Organization
Issuing authority of the PKD participant	PKD participant
Representative of PKD participant	PKD participant
ICAO PKD Operator	ICAO
ICAO PKD Officer	ICAO

4. What needs to be done prior to key ceremonies

4.1. Prior to first key ceremony after the participant joined the PKD

Certain information is required to be gathered before the first CSCA certificate(s) can be imported into the ICAO PKD System. With the following information, we can proceed with the key ceremony:

Please find below the prerequisites before the CSCA Import by means of a Key Ceremony can be performed:

Activities prior to first key ceremony after the participant joined the PKD			
Step	**Who**	**Activity**	**Status**
1	**Issuing Authority of the PKD participant**	Complete the “Notice of Participation” form and send it to the Secretary General of ICAO. Submit payment of the registration fee invoice prepared by ICAO in advance of the key ceremony.	☐ Done ☐ Open
2	**Issuing Authority of the PKD participant**	Complete the “Registration form for Participation in ICAO PKD” as in Attachment B of *ICAO PKD Regulations & Procedures* document.	☐ Done ☐ Open
3	**Issuing Authority of the PKD participant**	The CSCA certificate shall be checked for conformance to the ICAO standards by the participant by the means of the ICAO PKD conformance web-	☐ Done ☐ Open

		site. In case of issues with the certificates the participants should contact the PKD support of Veridos via the PKD online support system (preferred) or via email (pkdsupport@veridos.com) for assistance.	
4	**Issuing Authority of the PKD participant**	If conformance is confirmed, the participant submits the CSCA certificate(s) along with the electronic fingerprint to ICAO. A secure electronic transfer medium should be chosen. Participants also need to submit the following information about their representative who will be present at ICAO HQ in Montreal to hand over the CSCA certificate during the key ceremony (e.g. by providing a copy of the ID document – Passport/ID card) • Sex • Title • First name • Last name • Date of birth • Email • Type of ID for identification (ID card or Passport) • Number of ID document • Expiration date of ID document This information will be used to verify the identity of the participant's representative and recorded in the documentation confirming completion of the ceremony.	☐ Done ☐ Open
5	**ICAO PKD Operator**	The ICAO PKD Operator accesses the PKD system with smart card authorization. The submitted CSCA certificate is registered in the PKD system, the conformance against the ICAO standards is checked by the PKD system and the personal data of the announced representative is	

		entered and saved.	
6	**ICAO PKD Operator** **Representative**	After successful registration of the CSCA certificate(s) the appointment for the key ceremony at ICAO HQ in Montreal to import the CSCA certificate(s) is made by ICAO in agreement with the representative.	

4.2. Prior to key ceremonies to renew CSCA certificates (re-keying)

Each re-keying to a new CSCA shall be announced 90 days in advance to ICAO and forwarded for import at least 30 days in advance of actual use by the participant.

4.2.1. Self-signed CSCA certificates

If the participant is going to renew a CSCA certificate by a self-signed CSCA certificate the process requires a personal hand-over of the new CSCA certificate during a key ceremony at ICAO in Montreal by an authorized representative of the participant state. Prior to the key ceremony the following steps need to be done:

Activities to renew a CSCA by a self-signed CSCA certificate			
Step	**Who**	**Activity**	**Status**
1	**Issuing Authority of the PKD participant**	The CSCA certificate shall be checked for conformance to the ICAO standards by the participant by the means of the ICAO PKD conformance website. In case of issues with the certificates the participants should contact the PKD support of Veridos via the PKD online support system (preferred) or email (pkdsupport@veridos.com) for assistance.	☐ Done ☐ Open
2	**Issuing Authority of the PKD participant**	If conformance is confirmed, the participant submits the CSCA certificate(s) along with the electronic fingerprint to ICAO. A secure electronic transfer medium should be chosen. Participants also need to submit the following infor-	☐ Done ☐ Open

		mation about their representative who will be present at ICAO HQ in Montreal to hand over the CSCA certificate during the key ceremony (e.g. by providing a copy of the ID document – Passport/ID card): • Sex • Title • First name • Last name • Date of birth • Email • Type of ID for identification (ID card or Passport) • Number of ID document • Expiration date of ID document This information will be used to verify the identity of the participant's representative and recorded in the documentation confirming completion of the ceremony.	
3	**ICAO PKD Operator**	The ICAO PKD Operator accesses the PKD system with smart card authorization. The submitted CSCA certificate is registered in the PKD system, the conformance against the ICAO standards is checked by the PKD system and the personal data of the announced representative is entered and saved.	
4	**ICAO PKD Operator** **Representative**	After successful registration of the CSCA certificate(s) the appointment for the key ceremony at ICAO HQ in Montreal to import the CSCA certificate(s) is made by ICAO in agreement with the representative.	

4.2.2. CSCA certificates with corresponding CSCA Link certificate

If a participant wants to renew the CSCA certificate in the PKD system by applying CSCA Link certificates, both the new CSCA root certificate and the corresponding CSCA Link certificate, are submitted to ICAO for the key ceremony.

New CSCA certificate with corresponding CSCA Link certificate is the recommended choice to provide a new CSCA in case of re-keying. The personal presence of a designated representative during the key ceremony is not necessary in this case.

Activities prior to renewal of CSCA with CSCA Link certificate			
Step	**Who**	**Activity**	**Status**
1	**Issuing Authority of the PKD participant**	The CSCA certificate and the corresponding CSCA Link certificate shall be checked for conformance to the ICAO standards by the participant by the means of the ICAO PKD conformance website.	☐ Done ☐ Open
2	**Issuing Authority of the PKD participant**	If conformance is confirmed, the participant submits the CSCA certificate(s) and the CSCA Link certificate(s) along with the electronic fingerprint(s) to ICAO. A secure electronic transfer media should be chosen.	☐ Done ☐ Open

The key ceremony with import of the new CSCA and CSCA Link certificates into the HSM does not require the presence of a representative of the participant state.

5. What is done during key ceremonies

5.1. Key ceremonies with self-signed CSCA certificates

These key ceremonies are performed with an authorized representative of the participating state present during the ceremony. The key ceremony is comprised of the following steps:

Activities at key ceremonies for self-signed CSCA certificates		
Step	**Who**	**Activity**
1	**ICAO PKD Officer**	The representative's identity is checked by ICAO.
2	**Representa-tive**	The representative of the participating state is handing over the CSCA certificate and the corresponding electronic fingerprint on a USB storage device.
The key ceremony and the import of the CSCA certificate is done by two different author-ized ICAO PKD representatives:		
3	**ICAO PKD Operator**	An ICAO PKD Operator is accessing the PKD system with smart card authorization and is initiating the import of the CSCA certifi-cate into the HSM. This includes uploading the CSCA certificate, comparison with the previously registered certificate and finger-print, the conformity check of the CSCA certificate to the ICAO standards, and the entered personal data of the present repre-sentative of the participant state.
4	**ICAO PKD Officer**	An ICAO PKD Officer is accessing the PKD system with smart card authorization and confirms the correctness of all entered data and authorizes the import of the CSCA certificate into the HSM.

5	**ICAO PKD Operator** **ICAO PKD Officer** **Representative**	The ICAO PKD Operator prints the Key Ceremony Protocol documenting the relevant information about the imported CSCA certificate, the representative of the participating state and the executing ICAO PKD Operator and Officer. The protocol is then signed by ICAO and the representative of the participating state.

5.2. Key ceremonies for CSCA certificates with corresponding CSCA Link certificate

These key ceremonies are performed only by ICAO on behalf of the participating state. It is not required for a representative of the participating state to be present during the ceremony. The key ceremony is comprised of the following steps:

Activities at key ceremonies with CSCA Link certificates		
Step	**Who**	**Activity**
1	**ICAO PKD Operator**	The submitted CSCA certificate and the corresponding CSCA Link certificate are copied on a USB storage device and transferred to the operation workstation of the ICAO PKD.
The key ceremony and the import of the CSCA certificate and the corresponding CSCA Link certificate is done by two different authorized ICAO PKD representatives:		
2	**ICAO PKD Operator**	An ICAO PKD Operator is accessing the PKD system with smart card authorization and is initiating the import of the CSCA certificate to the HSM. This includes uploading the CSCA and CSCA Link certificates, comparisons with the previously registered certificates and fingerprints, and the conformity check to the ICAO standards.
3	**ICAO PKD Officer**	An ICAO PKD Officer is accessing the PKD system with smart card authorization and confirms the correctness of all entered data and authorizes the import of the CSCA and CSCA Link certificates into the HSM.

4	**ICAO PKD Operator** **ICAO PKD Officer**	The ICAO PKD Operator prints the Key Ceremony Protocol documenting the relevant information about the imported CSCA certificate, the CSCA Link certificate, and the executing ICAO PKD Operator and Officer. The protocol is then signed by ICAO.