For Publication on the ICAO Website

Guidance Document Migrating Country Signing Certification Authority (CSCA)

April 2018

File: Guidance Document Migrating Country Signing Certification Authority (CSCA)

Author: Subgroup of the New Technologies Working Group (NTWG), Working group of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)

Table of contents

1. PREPARATION FOR CSCA AND PKI MIGRATION 4

1.1 INTRODUCTION 4
1.2 PREPARATION 5
1.3 TIMING 5

2. GUIDANCE FOR DESIGNING THE NEW CSCA AND CORRESPONDING PKI 6

2.1 CONTACT INFORMATION 6
2.2 DOCUMENTS FOR OPERATION OF THE CSCA 6
2.3 FIELD CERTIFICATE POLICY 6
2.4 CHOICE OF ALGORITHM 6
2.5 SUBJECT ALTERNATIVE NAME / ISSUERALTNAME 6
2.6 MANAGEMENT OF ISSUED CERTIFICATES 7

3. GUIDANCE FOR DESIGNING THE BACK END OF THE NEW CSCA AND CORRESPONDING PKI 8

3.1 CA-SOFTWARE 8
3.2 SECURITY ISSUES 8

4. GUIDANCE FOR THE TRANSITIONAL PERIOD 9

4.1 CRLS 9
4.2 NEW CSCA CERTIFICATE 9
4.3 LINK CERTIFICATES 10
4.4 MASTER LISTS 11
4.5 DEVIATION LISTS 11
4.6 DECOMMISSIONING OLD CSCAS 12

5. ANNEXES 13

5.1 PROPOSED PLANNING FOR MIGRATION 13
5.2 CHECKLIST 14

History of changes

Date	Change	Name
28.06.2016	Re-issuance of SubCA certificates and Lists “Certificate Policy” “Proposed planning for migration” Proposal for new structure	Alban Feraud
03.08.2016	Multiple editorial changes in wording	Alan Bennett
16.09.2016	“CA-Software” editorial changes – acceptance of changes, adopting the new structure proposed by Alban Feraud	Kerstin Schönherr
29.09.2016	Rephrasing of Introduction Changes regarding LU comments	Kerstin Schönherr/Nicolas Thenée
09.11.2016	Insertion of contributions of ISO WG3. Answering of open comments.	Kerstin Schönherr/ Nicolas Thenée
03.03.2017	Resolutions of comments; improvement of wording	Nicolas Thenée / Thomas Schnattinger
04.04.2017	Resolution of comments; Adding of additional description and a figure describing re-keying of Root-CAs	Nicolas Thenée/ Thomas Schnattinger
21.02.2018	Clean version for TAG	Jens Bender
05.03.2018	Comments from veridos	Jens Bender

1. Preparation for CSCA and PKI migration

1.1 Introduction

This paper gives a technical and organizational guidance how to handle the migration from multiple CSCAs within one state to a single CSCA as recommended for the eMRTD PKI.

This guidance shall provide help IF a State migrates from multiple CSCAs to one single CSCA.

Note: Why migration should be done

> The eMRTD PKI was designed on the principle that "each issuing State/Authority establishes a single CSCA as its national trust point in the context of eMRTDs." (see Doc 9303-12, clause 3). This means trust within this CA is directly linked to the State;
>
> Therefore, "the eMRTD PKI is much simpler than more generic multi-application PKIs such as the Internet PKI defined in [RFC 5280]" and "PKI standards define a large set of optional features and complex trust relationships among CAs that are not relevant to the eMRTD application." (see Doc 9303-12, clause 2).
>
> Because of this, establishing more than one CSCA for one State leads to multiple problems when participating in the eMRTD PKI:
>
> More CSCA certificates need to be exchanged for multiple CSCAs, which increases the effort for the exchange and leads to the following question: Who is in charge and trustable for exchanging the CSCA certificates with the other States, if different agencies are responsible for the different CSCAs in one State?

1. Multiple CSCAs mean multiple contacts for foreign States concerning the eMRTD PKI. For example: If an unknown CSCA certificate occurs at the border control, who shall be contacted at the issuing State in the case the IssuerAltName does not help (e.g. the certificate is malicious)? Who is in charge for malicious certificates at the issuing site? Receiving States do not know if they have collected all different CSCA certificates from a State, therefore they are not able to ask for missing CSCA certificates.
2. Receiving countries expect Document Signer Certificates (DSCs) from one CSCA per State. If DSCs from additional CSCAs are issued, they may be suspected to be not authentic when they are received for the first time.
3. The Certificate Revocation Lists (CRLs) of the eMRTD PKI are designed to list revoked certificates by State. When multiple CSCAs exist, the border control has to check multiple CRLs for each eMRTD. Publishing only one CRL for different CSCAs leads to difficulties, as there is no way to indicate which CSCA has issued a revoked certificate as the indication of the certificates is State based. A similar issue occurs also for deviation lists and master lists if multiple CSCAs are operated.

1.2 Preparation

The first step is to get an overview of the current status regarding the number and characteristics of the CSCAs. Therefore, a list of all valid CSCA, Document Signer and Master list Signer certificates and all other certificates issued by each CSCA and their CRLs, including their validity periods and algorithms, should be prepared. The issue of governance shall also be clarified, i.e. defining the responsible entity as well as the governance and management rules (applicable certificate policy and certificate practice statements).

The following questions should be answered:

a) How many CSCAs are operational? Who is in charge of each CSCA?

b) Identify the entity(ies) in charge of each CSCA and define (1) a single entity to be in charge of the general CSCA management and (2) define common governance and management rules.

c) How many CSCA certificates of your State are still valid and published? There may be many times more CSCA certificates than CSCAs as the validity periods of CSCA certificates are up to 15 years, thus there are several valid CSCA certificates of one CSCA in parallel.

d) How long is the validity period of each CSCA certificate? The latest end of validity is the most important one; it will be the benchmark for the migration being finalized.

e) Do all CSCAs support similar algorithms and key lengths?

f) Keeping one of the CSCAs or implementing a new one? In each case, a new CSCA certificate should be issued including all the necessary link certificates.

g) Are the link certificates issued for all old CSCA certificates still valid?

h) Do all CSCAs issue Document Signer certificates and/or other certificates (e.g. Master List, Deviation List)?

i) What adaptations are required on systems that were using the old CSCAs? The adaptations which are required to migrate from old CSCAs to a single one is described in section 3.

1.3 Timing

Timing means the timing of the migration process. A time schedule for the different actions explained in the following paragraphs should be prepared.

The production cycles of the eMRTDs, deviation lists and master lists of CSCA should be included in the migration time schedule to minimize the risk of a production break.

2. Guidance for designing the new CSCA and corresponding PKI

The following paragraphs show how to solve the problems of multiple CSCAs by migrating the multiple CSCAs to one CSCA.

For this, the CSCA PKI must be rebuild considering the following aspects.

2.1 Contact Information

A single point of contact (person or organizational unit) of the migrating State shall be appointed for questions and problems of foreign States regarding the migration and operation of CSCAs..

2.2 Documents for operation of the CSCA

All other documents for the technical and organizational operation of the old CSCAs – especially the Certificate Policy, the CPS (see RFC 3647) and all documents which are public or mandatory for subscribers of the old CSCAs – shall be considered when establishing or revising those documents for the new CSCA. Among other definitions, they should strongly consider the CA's certificate policies in the definition of practices for issuance, publication, archiving, revocation and renewal of certificates and key pairs.

The final versions of these common documents (to be applied to the new single CSCA) need to be explicitly agreed upon by all managing bodies of each of the previous, multiple CSCAs.

2.3 Field Certificate policy

The field certificate policy **CertificatePolicies** is an optional field of the CSCA certificate that describes the governance and management rules applied by the issuing authority.

If it is used by the issuing authority and if (a) former value(s) was already defined and used with the former CSCA(s), a brand new value shall be assigned to replace the former certificate policies.

2.4 Choice of Algorithm

The different CSCA certificates may have been issued with different algorithms and key lengths. In this case, a decision must be made about which algorithm and key length shall be used for the new CSCA certificate. At least the strongest (i.e., cryptographically most secure) combination of algorithm and key length from the old CSCA certificates should be used for the new CSCA certificate. This will keep the level of security for all old CSCA certificates.

Note: An algorithm change from RSA to ECDSA or vice versa is not a problem provided that same security level is kept or exceeded.

2.5 Subject Alternative Name / IssuerAltName

The Subject Alternative Name/IssuerAltName is a mandatory parameter of the CSCA certificates which contains contact information for the issuing CSCA of the certificate.

If all old CSCA certificates contain the same Subject Alternative Name/IssuerAltName no special care needs to be taken. There is, however, an issue if the CSCA certificates from multiple CSCAs have multiple Subject Alternative/IssuerAlt Names. This problem has to be solved within the migration process.

Firstly, the Subject Alternative Name/IssuerAltName, i.e. the contact information, for the new CSCA has to be decided.

Secondly, the contact information represented by the Subject Alternative Name/IssuerAltName within the old CSCA certificates shall stay valid for the validity time of these certificates. This means communication attempts to the old contact points need to be forwarded to the new CSCA either manually or automatically within 5 working days.

2.6 Management of issued certificates

All certificates issued under one of the old CSCAs shall be newly issued with newly generated key pairs, when migrating to the new CSCA.

3. Guidance for designing the back end of the new CSCA and corresponding PKI

3.1 CA-Software

The software implementations managing the multiple CSCAs should be checked to ensure that they are capable of executing the following processes:

1. **CRLs**: The software of the new CSCA must be capable of importing DS, MLS, DLS and all other subordinate certificates of another CSCA and include those certificates into its CRL.
   Some implementations may require the import of the other CSCA certificates for this as well.
   Note: This does not mean to issue "indirect CRLs" according to RFC 5280 because the extension "CertificateIssuer" is not allowed according to ICAO Doc 9303-12 table 6 "CRL and CRL Entry Extensions Profile".
2. **Link certificates**: The software of each old CSCA must be able to import the new CSCA certificate and to issue a link certificate on it.
3. Issuing Master and Deviation lists containing certificates from other CSCAs

3.2 Security Issues

The security level of the CSCAs should be on the same level or higher for all keys and certificates even after the migration. Therefore, the Certificate Practice Statements or Security Concepts of the CSCAs should be compared to decide on the security mechanisms for the new single CSCA.

Some additional measures shall be conducted:

1. The repositories of all issued certificates and CRLs of the multiple CSCAs shall be copied to new CSCA or kept by the relevant old CSCA as long as the CSCA certificates are valid. This includes the copy of the whole certificate and registration databases and archived data according to the legislation of the Member States.
2. Private keys shall be kept until the CSCA link certificates signed by those keys are verified (internally and externally). The verification is done by
   a) checking the cryptographic signature of the CSCA link certificate generated with the private key of the corresponding CSCA certificate, and
   b) comparing the certificate information ("subject", "subjectPublicKeyInfo" and "SubjectAltName") of the CSCA link certificate to the certificate information of the new CSCA certificate[1].
3. The CSCA link certificates are distributed according to ICAO Doc 9303-12 chapter 4.2.3[2] for external verification. After successful verification, the private keys of the old certificates can be securely deleted.

[1] The verification can be done with standard PKI tools like openssl.

[2] 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

4. Guidance for the transitional period

4.1 CRLs

The Certificate Revocation List of a CSCA contains all certificates which are revoked by that CSCA, i.e. those certificates shall be considered to be not trustworthy anymore. The CRL must be published to everyone relying on the certificates managed by that CSCA.
The CRL shall be renewed at least every 90 days or when a certificate shall be revoked (refer to ICAO Doc 9303-12).

The certificates of the eMRTD PKI can be checked for their trust ability by checking the corresponding CRL by their two-letter country code and their serial number. This method expects unique serial numbers for the certificates of each State and a single CRL per State, otherwise this leads to revocation problems. If this case occurs, it has to be solved on step by step base.
Therefore, only the new CSCA certificate shall sign one single CRL. The CRL shall contain all entries of the CRLs of the old CSCAs and the CRL entries for the new CSCA. Entries of certificates issued by old CSCAs shall be included as long as the corresponding CSCA certificates are valid.
It can occur that multiple numbers of DS, DLS and MLS certificates are in use, because they are issued by different CSCAs. This is one of the problems caused by using multiple CSCAs within a single country.

Note: This does not mean to issue “indirect CRLs” according to RFC 5280 because the extension “CertificateIssuer” is not allowed according to ICAO Doc 9303-12 table 6 “CRL and CRL Entry Extensions Profile”.

How and where the CRL of a CSCA can be retrieved is noted by the CRL Distribution Point (CRL DP) as parameters in the CSCA certificate.
The new CSCA certificate will contain the CRL DP for its CRL, which contains all the revocation information of all old and new CSCAs, but the old CSCA certificates which are still valid still contain the old CRL DPs.

There are two options to solve this problem:

a. The CRL are published on the new CRL DP only and all other old CRL DPs redirect to this CRL DP.
b. The ONE CRL is published at each old CRL DP and at the new one.

The new CSCA shall receive revocation requests for the old CSCAs as long as old CSCA certificates are still valid.

4.2 New CSCA certificate

Certificates of the new single CSCA act, from the start of the migration, as the trust anchor of the State's eMRTD PKI system. Therefore, a new key pair should be generated and a new CSCA certificate should be issued, including the parameters based on the decisions made according to the paragraphs above.

Once a new CSCA certificate is issued, all the certificates of the PKI (DS, DLS, MLS,...) shall be reissued under the new CSCA and the certificates issued under the old CSCAs shall not be used anymore.

Note: The notification of planning to issue a new CSCA certificate has to be done at least 90 days in advance (ICAO Doc 9303-12, chapter 4.2.3[3]), but for the period between issuing and using a new CSCA certificate Doc 9303-12 states: "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".

4.3 Link certificates

CSCA certificates are self-signed as they are the trust anchor of a State's eMRTD PKI, i.e. all other eMRTD PKI certificates of that State can be cryptographically verified by using the CSCA certificate. Because of that reason, the first CSCA certificate of a State is exchanged with the other States in a trustable way using diplomatic channels.

The CSCA certificate has to be renewed including a new key pair every three to five years to uphold the level of security. In order to avoid the effort of diplomatic exchange with every new CSCA certificate, CSCA link certificates shall be issued4 by the CSCA, which can be used to cryptographically verify the authenticity and integrity of new CSCA certificates.

A CSCA link certificate contains the public key and the attributes of the new CSCA and is signed by the private key of the old CSCA certificate. Still, a chain of trust can be built from the new CSCA certificate of a State to its first one.

This mechanism of link certificates shall also be used for the migration from multiple CSCAs to a single CSCA in the following way:

- For each old CSCA certificate, whose private key usage period is not over yet, a CSCA link certificate shall be issued which contains the public key of the new single CSCA certificate and is signed by the corresponding old CSCA certificate. If the name of the old CSCA and the new CSCA differ, the link certificate must contain a `nameChange`-Extension as defined in Doc 9303-12.
- Note that in case of the revocation of one of the old CSCA certificates, the corresponding link certificate cannot be verified anymore, i.e. cannot be used anymore to verify trust in the new CSCA.
- When all CSCA link certificates have been issued, a complete trust chain ending up at the new CSCA certificate SHALL exist for each CSCA certificate still having a valid private key usage period.

Some of the old still valid CSCA certificates may not have a link certificate to the new CSCA certificate because their corresponding private key is not usable anymore. This problem must be countered by using Master Lists and Deviation Lists as described in the next clause. The following figure illustrates the above described process.

[3] 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.
[4] Doc 9303-12 clause 4.2.3 „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".

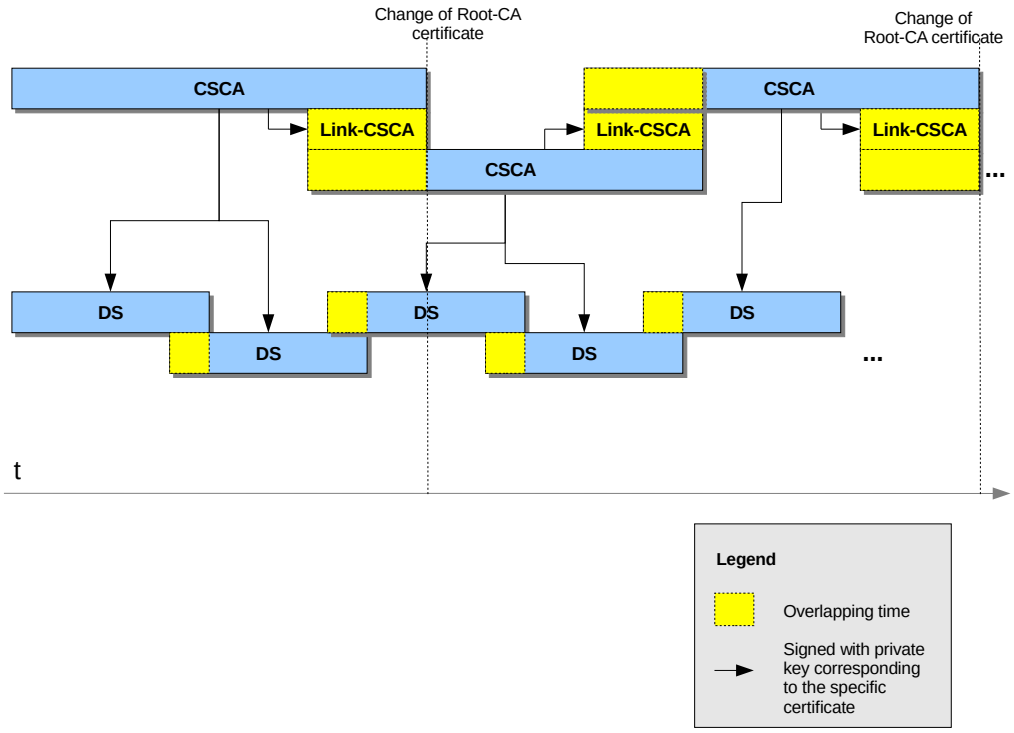


Figure 1: Re-keying process of CSCA certificates

4.4 Master Lists

Master lists are used to distribute CSCA certificates trusted by one CSCA. Usually, they are used to help in the distribution of foreign certificates, as well as older certificates of the same CSCA. In the context of migrating from multiple to a single CSCAs, we use the Master list to help receiving states to validate eMRTDs issued under the old CSCAs using the new CSCA certificate as the trust anchor.

A new Master list signer and a new Master list shall be issued in relation with the new CSCA. This Master list and the successive ones shall contain all CSCA certificates and link certificates that are still valid.

4.5 Deviation Lists

A Deviation List is issued by a State to specify non-conformities of travel documents and/or keys and certificates. The Deviation List has a defined format and is signed by the deviation list signer, using a certificate issued by the CSCA certificate.

A new Deviation list signer and a new Deviation list shall be produced. The Deviation List shall contain all old CSCA certificates that are still valid from the old CSCAs and the corresponding DS certificates in order to specify the non-conformity of multiple CSCAs.

So far no error code has been defined for the case of multiple CSCAs, a special error code for this case will be needed. At the moment, the generic deviation type **id-Deviation-CertOrKey**

can be used. This deviation type is specified as “A generic certificate or key related deviation not covered by the more detailed deviations below” (see Doc 9303-3, section 7.3.5).

4.6 Decommissioning old CSCAs

After everything mentioned in the clauses above has been finalized, the old CSCAs can be “terminated”, meaning completely removing the CA from operation, deleting all data and private keys from the systems and shutdown. This is also commonly known as “Decommissioning”.

This critical and complex procedure shall be planned well in advance and can only performed when it is guaranteed that the CSCA to be decommissioned is no longer needed for any further operations.

1. Execute the terms and procedures laid down in “CA and RA Termination” of the CPS (typically section 5.8 of CPS, if following the recommended outline of RFC 3647, chapter 6). For this, check carefully, that these terms and procedures do not contradict the measures listed in the clauses above (Clauses 1 – 4.5).
2. IMPORTANT: The migration of CSCAs and the corresponding decommissioning of the old CSCAs is NOT a reason to revoke any Document Signer certificates.
3. For each decommissioned CSCA, issue a final CRL. In line with Doc 9303-12, the `nextUpdate` field should not exceed 90 days. Responsibility for the revocation status of certificates by the decommissioned CSCAs is taken over by the single CSCA.
4. Evaluate the possible need to hold a full backup of the PKI, and store it safely under strictest custody and access rules.
5. Delete the old CSCA private key on the HSM as well as any backup copies according to the instructions of the HSM manufacturer.
6. If the hardware supporting the old CSCA (including servers, HSMs, backup tokens, activation tokens) is also decommissioned, zeroize it according to manufacturer instructions. As final step, electronic and physical destruction may be executed.

After completing all steps of the migration process, all records (documentation, forms, inventories, etc.) shall be properly archived for long term preservation, according to legal and policy requirements.

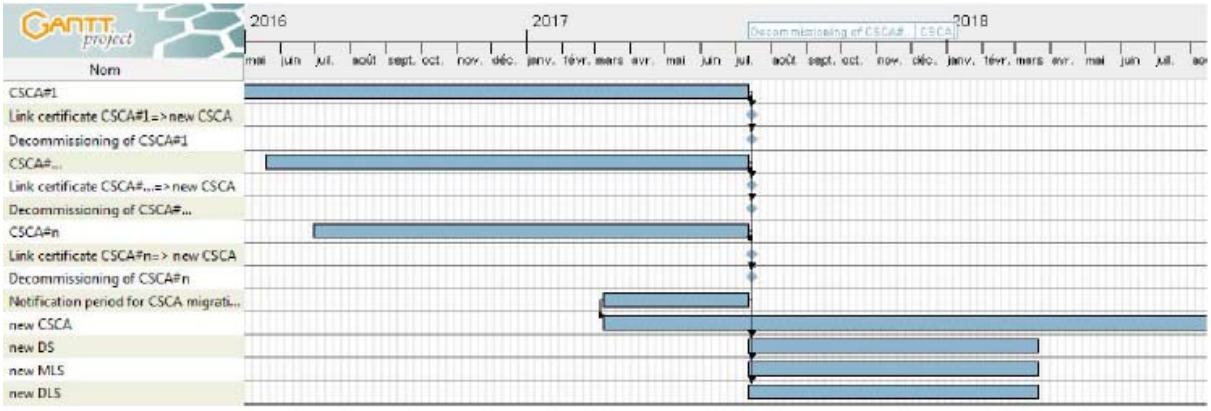
5. Annexes

5.1 Proposed planning for migration

This chapter aims at showing how to organize the CSCA migration. It is purely informative, and the dates and durations are purely provided for the illustration purpose.

Description:

- “CSCA#1” is the old CSCA whose expiration date is the earliest;
- “CSCA#n” is the old CSCA whose expiration date is the latest;
- “New CSCA” is the new single CSCA;
- “New DS” is the new Document Signer issued by the new CSCA;
- “New MLS” is the new Master List signer issued by the new CSCA;
- “New DLS” is the new deviation list signer issued by the new CSCA;
- “Link certificate CSCA#1 => new CSCA” is the link certificate of the “new CSCA” issued by “CSCA#1”;
- “Link certificate CSCA#n => new CSCA” is the link certificate of the “new CSCA” issued by “CSCA#n”;



5.2 Checklist

See Clause	TODO	DONE
Inventory		
1.2	List of CSCAs with name and responsible organization.	
1.2	List of issued CSCA certificates and technical characteristics per CSCA.	
1.2	List of issued certificates and CRLs still valid per CSCA.	
1.2	List of link certificates.	
1.2	Decision on new CSCA.	
1.2	Establishment of the entity responsible for the new CSCA, as well as of the governance and management rules.	
2.3	Decision on CertificatePolicies	
2.2	Decision on Certification Practice Statements	
2.4	Decision on the choice of algorithm for the new CSCA	
3.1	Check of CA-Software capabilities	
3.2	Determining on revision of security measures of new single CSCA, if applicable rearrange security measures	
1.3	Making a time schedule for the migration	
2.5	Decision on the Subject Alternative Names	
4.1	Decision on the CRL Distribution Points	
4.2	Issuing a new single CSCA certificate	
0	Issuing all needed link certificates	
4.1	Issuing a new CRL	
4.4	Issuing a new Master List	
4.5	Issuing a Deviation List	