Bundesamt
für Sicherheit in der
Informationstechnik

TR-03145-4

Secure CA operation, Part 4

Special requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) for the Extended Access Control of the German Official Travel Documents according to [TR-03110]

Version 1.1
11.02.2020

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: eID@bsi.bund.de
Internet: https://www.bsi.bund.de

Contents

1 Introduction

This document is part 4 of the Secure CA operation series of BSI TR-03145. The document series compiles requirements for Trust Center instantiating as Certification Authority (CA) in Public Key infrastructures (PKI) with a security level 'high'. Part 1 considers generic requirements for secure CA operation, while the other parts consider additional or modified requirements for specific exemplary business cases of PKI.

This document, part 4 of TR-03145, defines secure operation requirements being specific for Sub-CAs and Root-CAs of the Public-Key infrastructure (PKI) for the Extended Access Control of the German Official Travel Documents according to [TR-03110][1] in addition to or as replacement for some of the objectives and requirements of [TR-03145-1].

1.1 Scope and structure of this document

This document concerns the Root-CAs, called CVCA (Country Verifying Certificate Authority), and the Sub-CAs, called DV (Document Verifier), of the PKI for the Extended Access Control of the German Official Travel Documents, named CVCA-PKI in the following.

This document is part 4 of TR-03145 and contains necessary refinements and additions for the specific needs of CAs in the CVCA-PKI. Conformance to this document can only be reached by fulfilling all objectives and requirements of [TR-03145-1] which are not refined or discarded here in part 4 *and* the additional objectives and requirements of part 4.

Note: This document reflects requirements of the Root-CAs'[2] Certificate Policies of the CVCA-PKI in order to enable conformance to TR-03145 and the mentioned Certificate Policies as well, but it does neither replace nor comprise entirely the requirements of the Certificate Policies or regulations by law.

Clause 2 of this document contains three types of objectives and requirements:

- objectives and requirements from [TR-03145-1] refined for application in the CVCA-PKI. The new passages are marked with bold letters;
- lists of objectives and requirements from [TR-03145-1] which are not applicable in the CVCA-PKI. These are listed with their short term and number;
- objectives and requirements in addition to [TR-03145-1] to be used in the CVCA-PKI, they are defined next to the refined requirements and are labeled by extending the numbering of requirements with lower case letters, e.g. Renew.Req.8*a*..

The corresponding subclauses from [TR-03145-1] are highlighted in the titles of the subclauses.

Clause 3 is an Annex containing additional objectives and requirements which only concerns and is normative to those DVs issuing certificates for the eID application of the German eID scheme. Those DVs are called “BerCAs”.

1.2 Definitions

term	**definition**
CVCA-PKI	PKI for the Extended Access Control of the German Official Travel Documents according to [TR-03110].
CVCA	Country Verifying Certificate Authority, a Root-CA in the CVCA-PKI
DV	Document Verifier, a Sub-CA in the CVCA-PKI
BerCA	“Berechtigungs”-CA, a DV issuing certificates for the eID application (electronic identity) of the German eID scheme (see [TR-03110]).

Table 1: Definitions, abbreviations and notation

1 For an introduction to this special kind of PKI please refer to [TR-03110].
2 Namely the CVCA-eID, the CVCA-ePass and the CVCA-eSign.

2 Specific Requirements for Certificate Management Processes

2.1 Private key of the CA (clause 5.1 of TR-03145-1)

The following requirements of [TR-03145-1] concerning the private key of the CA are refined as stated below:

PRC.Req.1 The key pair generation of the **CVCA certificates and of the DVs initial certificates** shall be performed during a key ceremony in a four-eyes principle under attendance of the key responsible officer. For successive certificates of a DV this requirement needs only to be fulfilled, if the key generation process is initialized manually.

Application note: PRC.Req.9 only needs to be fulfilled if key backups are performed, which is not mandatory for DVs.

2.2 Certificate generation process (clause 5.5 of TR-03145-1)

The following requirements of [TR-03145-1] concerning the certificate generation process listed below are refined as follows:

CG.Req.3 The CA shall ensure, that the requesting subscriber is identified unambiguously, before starting the certificate generation process, **by checking the outer signature on a request for a successive certificate.** Additionally the CA shall check the correctness of the following information, which shall be included in the certificate:
1.) Certificate Authority Reference 2.) Certificate Holder Reference 3.) type of certificate 4.) public key corresponding to the private key under the subscriber control, 5.) period of validity, 6.) the certificate serial number, 7.) the electronic signature of the issuing authority, 8.) access rights 9.) certificate extensions (if applicable).

2.3 Revocation and suspension (clause 5.7 of TR-03145-1)

As revocation of certificates is not possible within the CVCA PKI, the option "*revocation*" in all objectives and requirements of clause 5.7 of [TR-03145-1] shall be ignored.

The requirements and objectives of [TR-03145-1] concerning revocation and suspension listed below are refined as follows:

RM.Obj.2 **The suspension process ensures** that subscribers which are no longer trustworthy (e.g. due to incidents in their IT Systems) are suspended by the CA **and they will not** receive any certificates as long as the suspension is active.

RM.Req.2 **The CA shall define an appropriate procedure for the suspension started by an authorized subscriber suspension. The involved parties and suspension reasons have to be clearly defined.** The CA shall ensure: 1.) the identification of persons/institutions with legitimate claim to apply for suspension of a subscriber: the subscriber/certificate holder, [assignment: *list of further persons/institutions*], 2.) the identification of reasons for a suspension: private key of certificate compromised, incorrect information on certificate, security incident on the IT systems of the certificate holder/subscriber, subscriber not fulfilling Terms and Conditions of the CA, [**assignment: other reasons for suspension**], **3.)** [**assignment: the transmission path and record of the suspension**] **4.)** [**assignment: additional requirements for a successful suspension**] **5.)** The suspension of a subscriber may only be canceled, if the cause for the suspension has been solved.

The following objectives and requirements of [TR-03145-1] do not apply for (Sub-)CAs affected by this document:

- RM.Obj.1
- RM.Obj.4
- RM.Req.3
- RM.Req.4
- RM.Req.5
- RM.Req.6

2.4 Certificate renewal, re-keying and update (clause 5.8 of TR-03145-1)

The CVCA CPs of the CVCA-PKI allow re-keying or update of a certificate issued for a certificate request based on a newly generated key pair, but do not allow renewal of a certificate.

As renewal of certificates is not allowed within the CVCA PKI, the option “renewal” in all objectives and requirements of clause 5.8 of [TR-03145-1] shall be ignored.

The requirements and objectives of [TR-03145-1] concerning certificate renewal, re-keying and update listed below are refined and extended as follows:

Renew.Obj.1 The CA shall provide an appropriate process for **re-keying and/or update** of a certificate if the process is requested by the subscriber or started by the CA. The CA shall ensure that the request is processed in a timely manner.

Renew.Req.8 The Root-CA shall ensure that the re-keying and/or update of the Root-CA certificate is processed in a timely manner, so that the creation of a link certificate between old and new Root-CA certificate is possible and the ability to issue revocation information signed by the Root-CA is always guaranteed.

Renew.Req.8a The Sub-CA shall ensure that the request for re-keying and/or update of the Sub-CA certificate is processed in a timely manner, so that the creation and the verification of an outer signature by the actual Sub-CA certificate on the request is possible.

The following objectives and requirements of [TR-03145-1] do not apply for (Sub-)CAs affected by this document:

- Renew.Req.4
- Renew.Req.5

2.5 Certificate Policy and Certification Practice Statement (clause 6.2 of TR-03145-1)

The following objectives and requirements of [TR-03145-1] do not apply for (Sub-)CAs affected by this document:

- CP.Req.3

Note: The security concept required by the CA's Certificate Policy may be part of the CPS.

2.6 Secured handling and storage of key material (clause 6.6 of TR-03145-1)

The requirement of [TR-03145-1] concerning secured handling and storage of key material listed below are refined as follows:

SHKM.Req.1 Private keys of the CA and, if applicable, of subscribers shall be **generated, held, used** and **deleted** in a security device following **the requirements of the Certificate Policy of the Root-CA** ensuring the claimed security features, including tamper resistance, side channel freeness, suitable access control, random number generator and security of cryptographic operations.

2.7 Maintained revocation status (clause 6.11 of TR-03145-1)

The objectives and requirements of [TR-03145-1] concerning maintained revocation status listed below are refined as follows:

MRS.Obj.1 The CA shall ensure **that suspension information are up-to-date and accessible by the registration and the certification processes as well.**

MRS.Req.1 The CA shall ensure that the maintained **suspension** information is secured against data lost, hardened against manipulation and updated in a period of [assignment: *number of hours*] hours in case of a revocation.

MRS.Req.3 The server hosting the maintained suspension information shall be hardened against failure and attacks. **The CA shall analyze the risk of a server failure and attacks against the server.** If necessary, the IT infrastructure shall be deployed redundantly.

The following objectives and requirements do not apply for (Sub-)CAs affected by this document:

- MRS.Req.2
- MRS.Req.4

2.8 Availability of services (clause 6.13 of TR-03145-1)

The objectives and requirements of [TR-03145-1] concerning availability of services listed below are refined as follows:

AS.Obj.1 The CA shall provide a **degree of availability of his services towards its subscribers tailored appropriate to the interval of certificate issuing.**

AS.Req.1 The CA shall define the maximal down time of each service and tailor the services appropriately. **Particularly the service treating the suspension of certificates shall ensure to process inquiries and updates within** [**assignment:** *number of hours*] **hours.**

2.9 CA termination (clause 6.14 of TR-03145-1)

The requirements of [TR-03145-1] concerning CA termination listed below are refined as follows:

CT.Req.2 The CA shall inform subscribers, subjects and **the Root-CA** as well as other entities the CA has agreements with successor instances (i.e. third party service providers) prior to it's termination. Therefore the process of the CA termination shall be described in the 'Terms and Conditions' as following sec. 5.2 of [TR-03145-1].

CT.Req.2a If a subscriber of a (Sub-)CA declares the termination of its business within the PKI, the subscriber has to be suspended by its CA at the termination date.

CT.Req.2b If a subscriber of a (Sub-)CA declares the termination of its business within the PKI, the last certificate which will be issued for that subscriber shall not have the end of validity beyond the termination date.

3 Annex: Revocation Service for the eID application[3]

The Revocation Service for the eID application is a process to prevent the misuse of the eID application with, for example, lost or stolen identity cards or residence permits. Therefore it only concerns BerCAs.

For details on the Revocation Service for the eID application please refer to [TR-03127].

For BerCAs, the following requirements apply in addition to those of [TR-03145-1]:

REVeID.Req.1a The BerCA shall install appropriate technical and organizational measure to ensure the confidentiality of the revocation token at all times.

REVeID.Req.2a The BerCA shall generate the key pairs for the revocation lists only within a security area fulfilling the following criteria: separated area, access control, access only for authorized personnel, ISO/IEC 27001 certificate covering the security area and the generation and use of the key pairs for the revocation lists.

REVeID.Req.3a The BerCA shall delete the outdated eID revocation list.

REVeID.Req.4a The BerCA shall compute its service specific revocation list based on DER encoding according to [ITU-T X.690].

3 Concerns BerCAs only.

Bibliography

ITU-T X.690	ITU-T. Information Technology: ASN.1 encoding rules: Specification of BasicEncoding Rules(BER), Canonical Encoding Rules (CER) and DistinguishedEncoding Rules (DER), X.690
TR-03127	BSI: Technische Richtlinie TR-03127 - Architektur Elektronischer Personalausweis und elektronischer Aufenthaltstitel
TR-03110	BSI: Technische Richtlinie TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS-Token
TR-03145-1	BSI: Technische Richtlinie TR-03145-1 - Secure CA operation, Part 1 - Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high'