



Federal Office
for Information Security

Certificate Policy of the German Country Signing Certification Authority (CSCA)

Version 2.0

14.11.24



Document history

Version	Date	Editor	Description
2.0	14.11.24	BSI	Revision of CP version 1.0 and updating to the current state of operation to a new version 2.0 of the CP. Insertion of internal comments.

Contents

	Document history.....	2
1	Introduction.....	5
1.1	Definitions.....	6
1.2	Overview.....	6
1.3	Document Name and Identification.....	7
1.4	PKI participants.....	7
1.4.1	Certification Authorities.....	7
1.4.2	Registration Authorities.....	7
1.4.3	Subscribers.....	8
1.4.4	Relying Parties.....	8
1.5	Policy Administration.....	8
2	Publication and Repository Responsibilities.....	9
2.1	Repositories.....	9
2.1.1	CSCA / CS-PKD.....	9
2.1.2	Publication of Certificates issued by the CSCA.....	9
2.1.3	N-PKD.....	9
2.1.4	ICAO-PKD.....	9
3	Identification and Registration.....	11
3.1	Naming.....	11
3.1.1	Naming Scheme of CSCA Root Certificate and Document Signer Certificates.....	11
3.1.2	Naming of Communication Certificates.....	11
3.1.3	Naming Scheme of Document Signer Certificates for Digital Seals.....	12
3.1.4	Naming Scheme of Master List-, Defect List- and Deviation List Signer Certificates.....	12
3.2	Initial Identification.....	12
4	Certificate Life-Cycle.....	14
4.1	Certificate Profiles.....	14
4.2	Initial Certificates and Requests.....	14
4.3	Re-Keying of Certificates.....	15
4.4	Certificate Application and Issuance.....	15
4.4.1	Requesting of Document Signer Certificates.....	15
4.4.2	Requesting of Master List-, Deviation List-, Defect List-Signer and Communication certificates.....	17
4.5	Certificate Acceptance.....	19
4.6	Certificate Usage.....	19
4.7	Certificate Validity Periods.....	19
5	Security Requirements.....	21
5.1	Physical Controls.....	21
5.2	Procedural Controls and System Access Management.....	21
5.2.1	Logging.....	22
5.2.2	Personnel.....	22
5.3	Incident Handling.....	22
5.3.1	Subscriber's Certificate Revocation.....	22
5.3.2	Incident and Compromise Handling Procedures.....	23
5.3.3	Entity Private Key Compromise Procedure.....	23

6	Key Pair Security.....	24
6.1	Key Pair Generation.....	24
6.1.1	Requirements for CSCA.....	24
6.1.2	Requirements for Document Signer.....	24
6.2	Private Key Protection and Cryptographic Module Engineering Controls.....	24
6.3	Key Escrow, Backup and Recovery.....	25
	Bibliography.....	26
	Keywords and Abbreviations.....	27

Tables

Table 1:	Common Name for Document Signer Certificate for non-electronic documents.....	12
Table 2:	Optional extensions according to [Doc 9303-12], which SHALL set in all certificates issued by the German CSCA.....	14
Table 3:	Generation of Document Signer certificate requests.....	17
Table 4:	Request of Master List-, Deviation List-, Defect List-Signer and Communication certificates.....	18
Table 5:	Private Key Usage Period and maximum Certificate Validity Periods for certificates issued under the CSPKI.....	20

1 Introduction

This document describes the Certificate Policy (CP) under which certificates of the German Country Signing Certification Authority (CSCA) are issued. The German CSCA is the Root Certification Authority of the German Country Signing Public Key Infrastructure (CSPKI) that is used to ensure the authenticity of German electronic official documents.

The CSCA issues certificates to manufacturers of German electronic machine-readable travel documents (eMRTDs), eID documents and official non-electronic documents with a digital seal. In Germany the following documents are issued:

- Passport (elektronischer Reisepass, ePass),
- German identity card (Personalausweis, PA)
- Residence permits (Aufenthaltstitel, eAT)
- eID cards for union citizens (eID-Karte für Unionsbürger, UB)

official non-electronic Document with digital seal:

- Arrival Attestation Document (Ankunftsnachweis, AAD)
- Address-Sticker for German Identity Card and Passports (Adress-Sticker, AS)
- Visa Sticker (Visa-Sticker, VS)

eMRTDs and eID documents are official identity documents containing a contactless chip that enables the storage of digital data. An official non-electronic document (e.g. Arrival Attestation Document or Visa sticker) is a paper based document containing a digital seal (see [TR-03137-1]).

The issuance of eMRTDs is in accordance with the European Council Regulation and PAuswG for PA on standards for security features and biometrics in travel documents ([EC2252]), which was adopted by the member states of the European Union in December 2004.

The digital data stored on eMRTDs and eID documents can be read and written by the use of terminals. These terminals are operated to communicate with the contactless chips of the eMRTDs and eID documents. The communication between the contactless chip and terminal is implemented using cryptographic protocols, called Extended Access Control (EAC) according to [TR-03110] in order to realize secure (i.e. encrypted and integrity protected) and authorized read and write access. For obtaining read or write permission on the contactless chip authorization certificates (see [TR-03110]) are needed.

Data stored on contactless chips of eMRTDs, eID documents and on official non-electronic documents with digital seal is (partially) digitally signed by the document manufacturer during the production process using the corresponding Document Signer private key. The terminals can use the corresponding Document Signer Certificates to check these signatures in order to verify the authenticity of the data stored on the eMRTDs, eID documents and official non-electronic documents with digital seals.

This CP sets forth the business and technical requirements for approving, issuing, managing, using, revoking and renewing certificates for manufacturers of German eMRTDs, eID documents and official non-electronic document with digital seal (Document Signer Certificates), for the operator of the national public key directory (N-PKD) issuer of (Master List-, Defect List- and Deviation List Signer certificates) and for client- and server based communication partners in the context of exchange of card verifiable certificates using communication (COM) Certificates. The operations and policies for these three types of certificates differ in some areas. In these cases, the concerning operations and policies are specified separately.

Requirements define the operation of CSPKI which ensures the integrity and authenticity of German eMRTDs and eID documents, Master Lists and communication processes. This policy is therefore targeted at both manufacturers of and entities relying on German official documents and eID documents. Its policy-

defining authority is the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik).

1.1 Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

1.2 Overview

The CSPKI consists of the following two entities:

1. Root-CA: The Country Signing Certification Authority (CSCA) operated by the Federal Office for Information Security (BSI),
2. Subscribers: The entities that are receiving certificates by the CSCA. These entities are:
 - The German Document Signer (DS) operated by the manufacturer of eMRTDs, eID documents and non-electronic documents with digital seals.
 - The N-PKD is an organizational unit, that is responsible for generation of Master Lists, Defect- and Deviation Lists
 - Communication side for SPOC communication

This means that the CSPKI is only composed of one CA. Thus, the CSCA directly issues subscriber certificates (see section 1.4.3). All issued certificates by the CSCA are of the type X.509. The CSCA certificates are stored as trust anchors in terminals reading eMRTDs and eID documents.

The CSCA issues the following types of certificates:

1. Document Signer certificates (DSC) are used to verify signed datagroups on the contactless chip, during the passive authentication, according to [TR-03110] and to verify the integrity and authenticity of digital seals of non-electronic documents (see [TR-03137-1]). The DSCs are issued by the CSCA, i.e. the CSCA Root certificate is used to verify the signature of the DSC.
2. The Master List Signer certificate is used to verify the signature of the Master List, that is generated with the private key corresponding to the Master List Signer certificate. The Master List described in [Doc 9303-12] is a signed list that contains all CSCA Root- and CSCA-Link certificates and the Master List Signer certificate, that is used to verify the signature of the Master List of a specific country. The Master List is used to distribute the CSCA Root certificates and CSCA Link certificates, that are trusted by the Master List Signer to different countries.
3. The Defect List Signer certificate is used to verify signed Defect Lists. Defect Lists contain information about Document Signer certificates or eMRTDs and eID documents containing elements that do not precisely conform to the ICAO specifications. The DSCs encoded on the Defect List can be used for verification of signed data of eMRTDs and eID documents although there is a defect. The Defect List is only generated for national use.
4. The Deviation List Signer certificate is used to verify signed Deviation Lists. Deviation Lists contain information about DSCs or eMRTDs and eID documents of the issuing country, containing elements that do not precisely conform to the ICAO specifications. This Deviation List is obtained via the ICAO-PKD and is used by international authorities during the passive authentication. The Document Signer certificates encoded on the Deviation List can be used for verification of signed data of eMRTDs and eID documents although there is a defect.
5. COM certificates are used for trusted client and server based TLS communication between different SPOCs (Single Point of Contacts) for exchanging the card verifiable certificates according to

[TR-03129-1]¹ and [TR-03129-3] on national level and on international level according to [EU-CP]. A SPOC is a webserver, which is used to exchange card verifiable certificates (see [EU-CP]) with national and international authorities for enabling read or write access to data groups of the eMRTD and eID documents.

1.3 Document Name and Identification

The document at hand is the Certificate Policy (CP) of the German Country Signing Certification Authority:

- Title: Certificate Policy of the German Country Signing Certification Authority (CSCA)
- Version: 2.0
- OID: 0.4.0.127.0.7.3.1.1.1

This document may be downloaded from <https://www.bsi.bund.de/cscs>. Both the OID and the URL are included within the `CertificatePolicies`-extension of each certificate issued under this policy.

1.4 PKI participants

This section gives an overview of the Certification Authority, Certificate Holders, Registration Authority, and Relying Parties of the German Country Signing Public Key Infrastructure. This PKI is part of the international security infrastructure to ensure and verify integrity and authenticity of German eMRTDs, eID documents and official non-electronic documents with digital seals.

1.4.1 Certification Authorities

The German CSPKI consists of only one Certification Authority (CA), the Root CA. It is called the German CSCA. The CSCA and the national public key directory (N-PKD) are operated by the BSI. The public keys of the German CSCA are contained in self-signed CA certificates called German CSCA Root certificates. The underlying certificate format is X.509 as described in [RFC5280].

The German CSCA issues certificates directly to the subscribers. The CSCA is responsible for:

- Technical verification, i.e. integrity and authenticity of the subscribers certificate request
- Issuing and publication of Certificate Revocation Lists (CRLs)
- Issuing the subscriber's certificate (see section 1.4.3)

1.4.2 Registration Authorities

There is one Registration Authority (RA) in the German CSPKI, the German Country Signing Registration Authority (CSRA). The CSRA is responsible for managing organizational and coordinative tasks.

The CSRA is located at the BSI. Certificate requests may be sent to the German CSRA by the contact given in Section 1.5

The German CSRA is responsible for performing:

- clear identification and authentication of the subscriber
- communication and coordination with the subscriber and the CA
- checking, if all organizational requirements are fulfilled (see section 4.4.1).

1 For Overlapping period of using the new version of TR-03129-1 and TR-03129-3 see https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03129/TR-03129_node.html

- checking the legitimacy of requesting certificates
- checking the issued certificate and its parameters, before sending it to the subscriber
- defining requirements and procedures for CSCA operation and updating of this CP and internal documentation

1.4.3 Subscribers

The subscriber is the holder of a certificate and in possession of its corresponding private key. The subscriber is clearly identified by the name in the certificate.

Subscribers under this policy are:

- German DS (i.e. manufacturers of German eMRTDs, eID documents and non-electronic documents with digital seals),
- the N-PKD (as the publisher and distributor of Master Lists, Defect Lists and Deviation Lists), and
- the communication side (TLS client- and TLS-server certificates) for SPOC communication.

1.4.4 Relying Parties

Relying Parties verify the authenticity and integrity of the data that is stored on eMRTDs, eID documents and on non-electronic documents with digital seals issued by a DS. Thus, in the context of this policy, Relying Parties only make use of certificates issued by the German CSCA -- they do not apply for certificates at the German CSRA. During the passive authentication, relying parties that are verifying the signed data groups, need to built up the certificate chain by using the corresponding DSC up to the CSCA certificate, that issues the DSC. Relying parties are e.g. terminals at border control or eID servers according to [TR-03130].

1.5 Policy Administration

This Certificate Policy is written, maintained and accounted for by:

- Organisation: BSI
- Address: Godesberger Allee 87, 53175 Bonn
- E-Mail: csc-germany@bsi.bund.de
- Website: <https://www.bsi.bund.de/csc>

Each update of this Certificate Policy will be published at <https://www.bsi.bund.de/csc> accordingly.

Further documents of the CSCA as the Certificate Practice Statement (CPS), security concept or operational concepts are internal documents which will be included for audits, but not be published. These documents adhere the requirements of the CSCA CP.

2 Publication and Repository Responsibilities

2.1 Repositories

2.1.1 CSCA / CS-PKD

The BSI operates a central directory called CS-PKD. The CS-PKD is part of the CSCA. It contains all certificates and CRLs issued by the CSCA :

- CSCA Root Certificates,
- CSCA-Link Certificates,
- DSCs,
- Master List Signer Certificates,
- Defect List Signer Certificates,
- Deviation List Signer Certificates,
- Arrival Attestation Document (AAD)-Signer Certificate,
- Visa Signer Certificates (VIC),
- Address-Sticker Certificates for German Identity Card and Passports,
- COM Certificates, and
- CRLs.

2.1.2 Publication of Certificates issued by the CSCA

The following information are published at <https://www.bsi.bund.de/csc>:

- all CSCA Root certificates
- all CSCA Link-certificates
- the current CSCA Master List
- the current valid Deviation List
- the current CRL
- all AAD-Signer Certificates
- all Visa Signer Certificates
- all Address Signer Certificates for German Identity Cards and Passports

2.1.3 N-PKD

Master Lists, Defect Lists and Deviation Lists, that are necessary for inspection processes are generated by the the N-PKD. The N-PKD distributes the Master Lists, Defect Lists and Deviation List via the SPOC.

2.1.4 ICAO-PKD

International certificate exchange is realized by the public key directory of the ICAO. The ICAO-PKD distributes, DSCs, CRLs, Master Lists and Deviation Lists (see [Doc 9303-12]) that are needed for verification

of the authenticity and integrity of the eMRTDs and eID documents to all receiving states. Additionally, the initial exchange of CSCA Root certificates is realized by bilateral diplomatic means for establishing trust.

3 Identification and Registration

3.1 Naming

Each issued certificate in the CSPKI MUST contain an issuer, identifying the signer of the certificate and the subject name, which identifies the public key of the certificate holder. The subject name for the certificates mentioned in chapter 2.1.1 must be unique within the CSPKI. For the CSCA Root certificate the issuer and subject name MUST be equal. In the following, the naming schemes of the certificates issued within the CSPKI are described:

3.1.1 Naming Scheme of CSCA Root Certificate and Document Signer Certificates

CSCA Root Certificate

The subject name MUST contain the following elements:

Country: C= DE

Organization: O =bund

Organization Unit: OU= bsi

Common Name: CN= cscs-germany

The Country name MUST be encoded as PrintableString and the value contains the format of two letter upper case country codes, as specified in [Doc 9303-3]. All other parameters are encoded as UTF8String.

Document Signer Certificates

The subject name MUST contain the following elements:

Country: C = DE

Organization: O = <Unique name of the legal entity>

Serial Number: SN= <Unique serial number of attribute type>

Common Name: CN = Document Signer <DocumentType>

The Country name MUST be encoded as PrintableString and the value contains the format of upper case two letter country codes, as specified in [Doc 9303-3]. The unique Serial Number must be encoded as PrintableString and is incremented for each issued certificate of one document type. Organization name and CN are encoded as UTF8String. DocumentType indicates the type of document for which the certificate is issued.

3.1.2 Naming of Communication Certificates

The subject name for the communication certificates MUST contain the following elements:

Country: C= DE

Organization: O =BSI

Common Name: CN= <SPOC TLS Client or Server>

Serial Number: SN= <Unique serial number of attribute type>

The Country name MUST be encoded as upper case characters in PrintableString format as specified in [Doc 9303-3]. The Serial Number must be unique and is incremented by each issued certificate issued for one document type, encoded as PrintableString. The parameter “O” and “CN” MUST be encoded as UTF8String.

3.1.3 Naming Scheme of Document Signer Certificates for Digital Seals

The subject name for Document Signer for digital seal are composed of the following elements as described in [Doc 9303-12]:

Country: C= DE: MUST be encoded as PrintableString

Common Name: CN: MUST consist of two uppercase characters, PrintableString format, that uniquely define the Bar Code Signer within one country. The table below lists the reserved Common Names for the Document Signer Certificates for digital seals as described in [TR-03137-1].

Document Signer Certificate	CN
AAD-Signer	ME
Visa Document Signer	VI
Address-Sticker Document Signer	ST

Table 1: Common Name for Document Signer Certificate for non-electronic documents

The Country (containing the format of two letter country code, see [Doc 9303-3]) and Common Name MUST be encoded as PrintableString with exactly two characters, defining the Digital Seal Signer within one country. Other parameters then the one described above are not allowed.

3.1.4 Naming Scheme of Master List-, Defect List- and Deviation List Signer Certificates

The subject name MUST contain the following elements:

Country: C= DE

Organization: O =bund

Organization Unit: OU= bsi

Serial Number: SN= <Unique serial number of attribute type>

Common Name: CSCA <Name of the List Signer>

The Country MUST be encoded with the two letter country code, see [Doc 9303-3]. The other parameters are encoded as UTF8String. The serial number MUST be unique and be encoded as PrintableString. The “CN” contains the name of the signer depending on the use case, encoded as UTF8String.

3.2 Initial Identification

The initial identity verification of a subscriber MUST be done by personal identification, verified by the CSRA of the CSPKI. The CSRA SHALL ensure the correct authentication of the subscribers by non-electronic means (e.g. verification of ID-document). In addition, the CSRA SHALL verify, if the subscriber is someone having specific rights, entitlements, or permissions (including the permission to act on behalf of the applying organization) to obtain a certificate.

If a responsible authority delegates the key management for signing to another entity, the delegating authority SHALL send a letter to the CSCA, approving this delegation. This letter MUST be submitted to the

CSCA before registration and issuing of DSCs. Without this approval a DSC SHALL NOT be issued for that use case.

4 Certificate Life-Cycle

4.1 Certificate Profiles

The certificates issued in the CSPKI are of the type X.509 according to [RFC5280]. The issuance and verification of the certificate SHALL be done via the shell model. For key pair generation, the requirements for cryptographic algorithm and key length of the latest version of [TR-03116-2] MUST be used.

The different certificates listed in section 2.1.1 are described in the following:

CSCA Root certificates, CSCA Link-certificates, Master List Signer-, Deviation List Signer-, Defect List Signer certificates, COM certificates and DSC fields SHALL be set according to the latest version of [Doc 9303-12]. All mandatory extensions according to [Doc 9303-12] SHALL apply. In addition to the mandatory extensions the following (optional) extensions according to [Doc 9303-12] MUST in addition be contained in all certificates:

Extension	Comment
AuthorityKeyIdentifier	Must be a SHA-160 hash value identifying the public key of the private key, which signs the certificate (see [RFC5280])
SubjectKeyIdentifier	Must be a SHA-160 hash value identifying the public key of the certificate holder (see [RFC5280])
CRLDistributionPoint	Must be http://www.bsi.bund.de/cscs_crl

Table 2: Optional extensions according to [Doc 9303-12], which SHALL set in all certificates issued by the German CSCA

For CSCA Root certificates, CSCA Link-certificates and DSCs (excluded Document Signer for digital seals) the included PrivateKeyUsagePeriod MUST contain the notBefore and notAfter values with validity period according to section 4.7. In addition, all certificates except the COM certificates and Document Signer for digital seal SHALL contain the Certificate Policy Identifier according to section 1.3. The other certificates that are issued by the CSCA SHALL NOT contain the PrivateKeyUsagePeriod Extension²

The COM (TLS client and server) certificates SHALL contain the KeyUsage extension with the value digitalSignature and keyAgreement. The SubjectAlternativeName extension MUST be present in the TLS-Server certificate. The ExtendedKeyUsage MUST be set to TLS Web ClientAuthentication for TLS client certificates and TLS Web Server Authentication for TLS server certificates. For COM certificates the requirements as defined in [TR-03116-4] SHALL be applied.

For Master List- and Deviation List Signer the ExtendedKeyUsage extension is according to [Doc 9303-12]. For DefectList Signer the ExtendedKeyUsage is: {itu-t(0) identified-organization(4) etsi(0) reserved(127) etsi-identified-organization(0) 7 applications (3) id-npki (11) id-defectExchange (2) id-electronicDefect (1) 2}.

The encoding of the AAD-Signer certificates, Visa Signer certificates and Address-Sticker Signer certificates SHALL be according to [TR-03137-1].

4.2 Initial Certificates and Requests

An initial certificate request is defined as:

- being the first certificate of the same certificate holder or
- being the first certificate after suspension or revocation or

² The private key usage period as defined in section 4.7 SHALL be ensured by organizational means in this case.

- being a new certificate after the previous certificate has been expired before a new request or link certificate is generated.

Initial certificates SHALL be issued based on PKCS#10 requests according to [RFC2986]. For each certificate request a new key pair SHALL be generated.

4.3 Re-Keying of Certificates

A successive or re-keying request is a certificate request of the same applicant (subscriber), who has already requested an initial certificate. A successive certificate SHALL only be issued under the following conditions:

- for each request a new key pair MUST be generated
- the validity of the certificate (or private key usage period) to be re-keyed, reaches the end of validity time and
- the integrity and authenticity of the re-keying request is verified³
- the certificate fulfills the requirements mentioned in section 4.4.

4.4 Certificate Application and Issuance

The CSCA SHALL take measures to ensure that the procedure of issuing the certificate is securely linked to the associated applicant.

4.4.1 Requesting of Document Signer Certificates

For issuing Document Signer certificates the following steps MUST be applied:

3 As long as the key Attestation functionality is not implemented, re-keying request are handled like initial requests. This means the requests are physically brought to the CSCA by the document manufacturer for identity verification and the steps described in section 4.4.1 SHALL be applied.

Step no.	Indication	Description	Party involved
1	Key Pair generation	The subscriber generates a key pair according to the requirements of [TR-03116-2] and section 6.1.	Subscriber
2	Generation of certificate request	The subscriber generates a PKCS#10 request, according to [RFC2986], out of the new generated public key considering the naming scheme of section 3.1.1. ⁴	Subscriber
3	Delivering the certificate request and additional information to the CSRA	<p>The PKCS#10 request is transferred by physically means to the CSRA for verification⁵. In addition, the following documentations SHALL be delivered previously via e-mail to the CSRA⁶:</p> <ul style="list-style-type: none"> • Identifier of the document type the Subscriber is applying for a DS certificate • A valid Common Criteria Certificate as well as TR-03105 certificate for the contactless chip of the eMRTD and eID document, for which the DSC is requested. • A number of reference samples for which the DS are constructed • a qualified signed PDF, submitted by the subscriber who has generated the request, which must contain the following information: <ul style="list-style-type: none"> - Filename of the Document Signer Request as agreed between CSCA and the subscriber. - SHA256-fingerprint of the Document Signer request for verification of the integrity of the request. - information on serial number and firmware of the HSM generating the request - Time, when the request was generated 	Subscriber/ CSRA
4	Verification of documentation	The CSRA verifies, if all the necessary information mentioned in step 3 is complete and valid and if the CSCA is allowed to issue the corresponding certificate.	CSRA
5	Verification of the Request	The CSRA verifies the identity of the Subscriber and the integrity and authenticity of the certificate request. If one of the checks fails, the request is rejected (return to step 1).	CSRA/ Subscriber
6	Issuance of the DS certificate	After positive feedback from the CSRA the CSCA issues the corresponding DSC	CSCA/ CSRA
7	Verification of DS certificate regarding cryptography and semantic	The CSCA sends the generated DSC to the CSRA for cryptographic verification and examination of semantic correctness. Afterwards , the CSRA notifies the CSCA of	CSCA/ CSRA

4 In the future, the HSM will be required to attest the document signer private key it generated. This will be done using a private attestation key, which follows the requirements as described in [ReqKeyAtt]. The attestation of the document signer private key is inserted as a PKCS#10 extension as defined in [KeyAttData].

5 The certificate request SHALL be delivered with a maximum period of 3 month in advance.

6 For Document Signer Certificates for Arrival Attestation, visa sticker, and address sticker no TR-03105 and CC certificate is required.

	correctness	the result.	
8	Send the DS certificate to the subscriber	The CSCA sends the generated DS certificate via email to the corresponding subscriber.	CSCA/ Subscriber

Table 3: Generation of Document Signer certificate requests

4.4.2 Requesting of Master List-, Deviation List-, Defect List-Signer and Communication certificates

This section describes the certificate request for the Master List Signer-, Deviation List Signer-, Defect List Signer certificates and communication certificates.

Step no.	Indication	Description	Party involved
1	Key Pair generation	The subscriber generates a key pair according to the requirements of [TR-03116-2].	Subscriber
2	Generation of certificate request	The subscriber generates a PKCS#10 request, according to [RFC2986], out of the new generated public key considering the naming scheme of section 3.1.4.	Subscriber
3	Delivering the certificate request	The PKCS#10 request is transmitted via email to the CSRA	Subscriber/CSRA
4	Verification of the Request	The CSRA verifies the identity of the subscriber and the integrity and authenticity of the certificate request. If the verification fails, the request is rejected, then start with step 1.	CSRA/Subscriber
5	Issuance of the certificate	After positive feedback of the CSRA, the CSCA issues the corresponding certificate	CSCA/CSRA
6	Send the certificate to the subscriber	The CSCA sends the generated DSC via email to the corresponding subscriber.	CSCA/Subscriber

Table 4: Request of Master List-, Deviation List-, Defect List-Signer and Communication certificates

4.4.2.1 CSCA Root Certificates

The CSCA generates its initial Root-CA key pair according to the requirements of the [TR-03116-2], inside the HSM (see section 6.1) and issues the corresponding self-signed certificate, according to ICAO [Doc 9303-12].

- CSCA Root certificate requests are done by the CSCA itself.
- Before the CSCA Root-CA key pair reaches the end of usage, a new (successive) CSCA Root-CA key pair **MUST** be generated.
- For the successive key pair a new CSCA Root and a CSCA-Link-certificates (see [Doc 9303-12]) **MUST** be issued. The corresponding CSCA-Link-certificate **MUST** be signed by the current active and valid CSCA Root-CA private key. Thus, the validity period of the CSCA-Link-certificate **SHALL NOT** exceed the validity period of the CSCA Root certificate used to verify the signature of the CSCA-Link-certificate.
- The initial CSCA Root certificate and all following CSCA Root and CSCA-Link-certificate **MUST** be used by the terminal reading the eMRTD and eID documents for performing passive authentication. For this case, the integrity and authenticity of the certificates **MUST** be ensured.

4.4.2.2 Application period and response time

The CSCA and CSRA **MUST** process the certificate requests within a timeframe of 5 working days⁷. In this case, the timeframe indicates the period of time from receiving the request to the issuance of the certificate. The response consists of:

- the delivery of the requested certificate (normal case)

⁷ Working days are days from Monday to Friday, excluding bank holidays, which are valid in Germany or North Rhine-Westphalia as well as “Rosenmontag” (carnival), the 24th December and the 31st December

- or a rejection and a description why the certificate is not issued.

The response is sent via email to the subscriber.

4.5 Certificate Acceptance

After receiving a requested certificate, the subscriber **MUST** check the correctness of the certificate. If the received certificate is not rejected by the subscriber within 3 working days of its delivery, the certificate is accepted. For rejecting a certificate the subscriber **MUST** write an email containing the reason, why the certificate is not accepted by the subscriber (e.g. the certificate contains an invalid field). The reason of rejection is checked by the CSCA.

4.6 Certificate Usage

For the CSCA, key pairs and certificates are used for the following purposes:

- CSCA Root-CA private keys **SHALL** be used to sign CSCA Root certificates, CSCA-Link-certificates, CRLs and the certificates listed in section 2.1.1. Thus, the CSCA Root certificate contains the KeyUsage extension with keyCertSign and cRLSign according to [RFC5280]. This extension **MUST** be set to critical.
- CSCA Root certificates **SHALL** be used to verify signatures of CSCA-Link-certificates, CRLs and the subscriber certificates listed in section 2.1.1.

DSCs are used to verify the signature of the datagroups on eMRTDs and eID documents. Master List-, Defect List- and Deviation List Signer are used to verify the signature of the corresponding issued list. Thus, all the DS (excluded the one for issuing digital seals), Master List Signer, Defect List Signer and Deviation List Signer private keys are only used for signing and the certificate encode “digital signature” as KeyUsage extension.

4.7 Certificate Validity Periods

The validity periods for the certificates issued in the CSPKI are described in Table 5.

Entity	Private Key Usage ⁸	Maximum Public Key Validity Period
CSCA Root certificate	3 years and 2 months	14 years 3 months
CSCA-Link-certificate	3 years and 2 months	End of validity of the signer certificate
Document Signer Passport	6 months	10 years and 6 months
Document Signer eAT	7 months	10 years and 7 months
Document Signer PA	7 months	10 years and 7 months
Document Signer UB	1 year and 1 month	11 years and 1 month
Master List Signer ⁹	1 year and 3 months	4 years
Deviation List Signer	1 year and 3 months	4 years

⁸ The Private Key Usage describes the maximum period, in which the entity is allowed to use its private key for signing operation. i.e. it **MUST** be ensured that new certificates are requested before the private key usage expires. After the private key usage period the old certificate **MUST** only be used for verification.

⁹ Master List Signer, Deviation List Signer, Defect List Signer, COM Certificates, AAD-Signer, Address-Sticker Signer and Visa-Signer certificates do not encode the private key usage period within the certificate. i.e. the Subscriber **SHALL** ensure that the private key is used according Table 5.

Defect List Signer	1 year and 3 months	4 years
Common List Signer	1 year and 3 month	4 years
COM certificates	1 year	1 year and 14 days
AAD-Signer	1 year and 2 months	2 years
Address-Sticker-Signer	1 year and 1 month	11 years and 1 month
Visa-Signer	1 year and 2 months	6 years and 2 months

Table 5: Private Key Usage Period and maximum Certificate Validity Periods for certificates issued under the CSPKI

5 Security Requirements

5.1 Physcial Controls

The CSCA SHALL ensure that it operates its services in a secure environment. This SHALL include:

- **Site location and construction:** The CSCA is operated in a physically protected area.
- **Physical access:** Access to the CSCA is controlled. Only authorized persons have physical access to the CSCA environment.
- **Media storage:** The storage media are protected against unauthorized or unintended use, access, disclosure or damage by people or other threats (e.g. fire, water).
- **Waste disposal:** Procedures for the disposal of waste are implemented in order to avoid unauthorized use, access or disclosure of sensitive data.
- **Off-site backup:** An off-site backup of critical data MAY be installed.

5.2 Procedural Controls and System Access Management

The CSCA SHALL implement security measures in order to protect the authenticity, integrity and confidentiality of their data and accurate functioning of their IT system. The CSCA SHALL have a security concept, which:

- lists any IT systems being part of the Certification Authority handling data for certification processes
- describes any process being part of the CSCA
- describes the roles and personnel needed
- describes security measures and incident handling
- describes the security measures for protecting the private key.

In addition the following item SHALL be covered:

- **Trusted roles:** Processes of CA and RA tasks SHALL be attached to trusted roles. At least the following roles SHALL be available: system administrator, auditor, RA operator and CA operator. This SHALL be realised by organisational measures as well as IT controls and SHALL include user account management, auditing and timely modification or removal of access.
- **Separation of trusted roles:** the IT system SHALL enforce sufficient computer security controls for separation of trusted roles. Distinct roles SHALL NOT be held by the same person. The CSCA and the CSRA SHALL be operated by different units within the BSI.
- **Access Control:** authentication of roles SHALL be enforced by the IT system for system access. Access to data or functionalities SHALL only be granted to trusted roles allocated to the corresponding task.
- **Two-person principle:** security critical tasks SHALL be implemented by a two-person principle.
- **Secure area:** the CSCA MUST be operated in a security area. Access to this area SHALL only be allowed for a limited number of authorized person. The persons having access to the security area MUST be mentioned in the security concept. This security area MUST be certified according to [ISO27001] based on BSI-IT-Grundschutz

- **Substitution concept:** for the case of unavailability of personnel covering trusted roles the substitution MUST be planned. Also in case of substitution a person SHALL not have the possibility to cover (multiple) separated roles.
- **Logging:** each modification of sensitive data SHALL be logged which includes private key operations.
- **Life-Cycle of security measures:** it MUST be ensured that the security measures are updated regularly during the life-cycle of the PKI.

5.2.1 Logging

The CSCA MUST implement appropriate logging mechanism to analyse the correct or incorrect usage of the system. The at least following events MUST be logged:

- the creation, deletion, using of private keys and certificates
- creation and modification of user roles
- the security incident reports and requests and the action taken.

The logs MUST be stored in an integrity and confidentiality protected way. Events are stored in a way that they can not be easily removed or modified.

5.2.2 Personnel

The following requirements SHALL be maintained concerning personnel of the CSCA:

- **Knowledge:** Personnel SHALL possess of the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function;
- **Reliability:** Personnel SHALL undergo domestic security screening appropriate to the role(s) they are carrying out.
- **Conflicts of interest:** Personnel SHALL be free from conflicts of interest;
- **Completing checks:** Personnel SHALL NOT have access to the trusted functions until any necessary checks are completed;
- **Clear instructions:** Personnel SHALL be clearly instructed on their duties and tasks;
- **Accountability:** Personnel SHALL be accountable for their activities.

5.3 Incident Handling

5.3.1 Subscriber's Certificate Revocation

The CSCA SHALL revoke the subscriber's certificate in the following cases:

- if any incidents such as private key compromise or security vulnerabilities, that endanger the security goal of the PKI, occur
- if the subscriber does not fulfill the requirements mentioned in the CP.
- If the Document Signer private key is used for any purpose that is not approved.
- Termination of participation in the CSPKI

Subscriber's certificates MUST be revoked via a CRL issued by the CSCA according to [Doc 9303-12]. Before a certificate is revoked, the CSCA MUST get the approval by the CSRA. The CRLs SHALL contain the

AuthorityKeyIdentifier and CRLNumber extensions (both extensions are non-critical). All other extensions are not allowed.

The CRLs MUST be regularly updated every 90 days. In addition, the CRL MUST be updated, if a new entry is inserted. In this case, the CRL MUST be issued within at least 48 hours, after the compromise has been reported to the BSI. The CSCA SHALL publish the CRL via a Distribution Point, which is encoded in the CSCA and subscriber certificates.

5.3.2 Incident and Compromise Handling Procedures

In case of a disaster, including the compromise of a private key, the CSCA and subscribers MUST ensure that operations are restored as soon as possible. In particular, the following requirements hold:

- The CSCA SHALL define and implement a continue plan to enact in case of a disaster
- CSCA systems data necessary to resume CSCA operations SHALL be backed up and stored in safe places suitable to allow the CSCA to return to operations in case of incidents/disasters in a timely manner.
- Backup and restore functions SHALL be performed by the relevant trusted roles
- The CSPKI business continue or disaster recover plan SHALL describe the compromise or the suspected compromise and the planned process.

If a private key of the CSCA or subscriber is unusable because of a key compromise, the reason why the compromise has occurred MUST be detected and resolved first. In case of a key compromise, the subscriber MUST inform the CSCA immediately and describe the security incident. The CSCA SHALL NOT issue any DSCs until the security incident is resolved.

After that, the CSCA or subscriber SHALL produce a new initial request as described in section 4.4.

5.3.3 Entity Private Key Compromise Procedure

A subscriber SHALL immediately inform the IT-situation centre of the BSI via meldungen-csca@bsi.bund.de and the CSCA (csca-germany@bsi.bund.de) of misuse and compromise of its private key. The CSCA SHALL revoke the subscriber's certificate and MUST stop issuing certificates for that revoked subscriber. The subscriber SHALL stop using that private key immediately. The incident report and solution of the security problem having caused the incident SHOULD be shared with the CSCA. After solving the security problem, the subscriber SHALL request an initial certificate.

6 Key Pair Security

6.1 Key Pair Generation

The requirements mentioned below are mandatory for the CSCA key pairs and all Document Signer key pairs used for signing eMRTDs eID documents and official non-electronic documents with digital seals.

6.1.1 Requirements for CSCA

The CSCA SHALL ensure the following requirements:

- the cryptographic module MUST be operated within the [ISO27001] certified security area of the Federal Office for Information Security, according to section 5.2.
- the key pairs MUST be generated according to the requirements of [TR-03116-2] and MUST fulfill security level 2 of [KeyLifeCycle]¹⁰.
- the CSCA SHALL ensure that the integrity and authenticity of their public keys are maintained during distribution to the subscribers.

6.1.2 Requirements for Document Signer

The DS SHALL ensure that their keys are:

- generated in a controlled and ISO/IEC-27001 certified environment according to section 5.2. The current valid ISO/IEC-27001 certificate MUST be submitted to the CSCA. The subscriber MUST have a valid ISO/IEC-27001 certification at all times.
- created in a certified and approved¹¹ cryptographic module, which SHALL fulfill all requirements of security level 2 of [KeyLifeCycle]
- generated according to [TR-03116-2]
- the DS SHALL ensure that the integrity and authenticity of their public keys are maintained during distribution to the subscribers.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private keys of CSCA and the subscribers MUST fulfill the following requirements:

- **Trustworthy device:** Private keys SHALL be held and used within the cryptographic module and SHALL only leave the cryptographic module for backup purposes, where section 6.3 applies.
- **Lifecycle of trustworthy device:** The trustworthiness of the device MUST be ensured during its lifetime, i.e. that the cryptographic module is not tampered with during shipment and operation.
- **Access control on trustworthy device:** For keys that are stored in cryptographic modules, access controls SHALL be in place to ensure that keys are not accessible outside the cryptographic module. In addition, there SHALL be measures to prevent unauthorized use of private keys.

¹⁰ The CSCA is allowed to approve exceptions for separate requirements

¹¹ The HSMs MUST fulfill all relevant national approvals needed for signing the datagroup of eMRTDs and eID documents.

- **Key destruction:** Private keys SHALL NOT be used after the end of their private key usage period (see section 4.7). All private keys and their backup MUST be securely deleted by the mechanism of the cryptographic module.

6.3 Key Escrow, Backup and Recovery

If key backup for the CSCA or Document Signer is done this MUST be done according to section 6.2 and the following requirements:

- Backup copies SHALL only be stored and used by a limited number of trusted personnel in a physically secure environment. The number of personnel carry out this function SHOULD be kept to a minimum. Backup copies of the private keys SHALL only be done with the functions provided by the cryptographic module in encrypted and integrity protected way. Backup copies SHALL only be imported and used in HSMs fulfilling the same security level according to [KeyLifeCycle] level 2. Backups of DS private keys SHALL only be imported in the HSMs of the same security level, operated in the security area of the document manufacturer¹².
- Backup copies SHALL only be used for restoration of the service of the cryptographic module.

¹² When the key attestation functionality is implemented the backup SHALL be done as described in Section 4 of [ReqKeyAtt].

Bibliography

- [Doc 9303-12] ICAO: Doc 9303 Machine Readable Travel Documents, sevens Edition, Part 12: Public Key Infrastructure for MRTDs ,
- [Doc 9303-3] ICAO: Doc 9303: Machine Readable Travel Documents, Part 3: Specifications Common to all MRTDs,
- [EU-CP] BSI: Common Certificate Policy for the Extended Access Control Infrastructure fro Travel and Residence Documents issued by EU Member States,
- [ISO27001] ISO/IEC: Information technology - Security techniques - Information security management systems - Requirements,
- [KeyAttData] BSI: Attestierung in eID-Infrastrukturen,
- [KeyLifeCycle] BSI: Key Lifecycle Security Requirements,
- [ReqKeyAtt] BSI: Anforderung an die KeyAttestation im Anwendungsfall der Attestierung von Document Signer Zertifikatrequests,
- [RFC2986] Network Working Group: PKCS#10: Certification Request Syntax Specification,
- [RFC5280] Network Working Group: RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,
- [TR-03110] BSI: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token,
- [TR-03116-2] BSI: Technische Richtlinie TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2: eID-Karten und hoheitliche Dokumente,
- [TR-03116-4] BSI: Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4: Kommunikationsverfahren in Anwendungen,
- [TR-03129-1] BSI: Protocols for Management of Certificates and CRLs in Public-Key-Infrastructures-Part 1: Common Specification,
- [TR-03129-3] BSI: Protocols for the Management of Certificates and CRLs in Public-Key-Infrastructures (PKIs)) -Part 3: Electronic Identity (eID) documents based on Extended Access Control (EAC),
- [TR-03130] BSI: Technical Guideline TR-03130 eID-Server,
- [TR-03137-1] BSI: Technical Guideline TR-03137: Optical Verifiable Cryptographic Protection of non-electronic documents (digital seal),

Keywords and Abbreviations

Abbreviations	Meaning
AAD	Arrival Attestation Document
CA	Certification Authority
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSCA	Country Signing Certification Authority
CSPKI	Country Signing Public Key Infrastructure
DS	Document Signer
eAT	Electronic residence Permit
eMRTD	electronic Machine Readable Travel Document
ICAO	International Civil Aviation Organization
ICAO PKD	ICAO Public Key Directory
ISO	International Organization for Standardization
N-PKD	National Public Key Directory
OID	Object Identifier
RA	Registration Authority
SPOC	Single Point of Contact
TLS	Transport Layer Security
VIC	Visa Signer Certificate