Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Certificate Policy für die Country Verifying Certification Authority eID-Anwendung

Elektronischer Identitätsnachweis und Vor-Ort-Auslesen mit hoheitlichen Ausweisdokumenten

Version 2.4
22. Juli 2021

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

Änderungshistorie

Version	Datum	Beschreibung
1.995	19.05.2015	vollständige Überarbeitung des Dokuments
1.996	01.07.2015	Einarbeitung der externen Kommentare: • Ergänzung: „Die Einzelheiten bezüglich der Aufgabenabgrenzung im Bereich RA zwischen BerCA und VfB regelt die VfB." • Korrektur: „Diensteanbieter-spezifische Sperrliste" zu „dienstespezifische Sperrliste" • Ergänzung: Fußnote 6 „Pseudonym = dienste- und kartenspezifisches Merkmal gemäß §2 Abs. 5 [PAuswG]" • Ergänzung: „Sofern die Extension zwei Sector Public Keys enthält (z.B. für eine Migration, siehe Kapitel 5.4.1), so MUSS der neueste Sector Public Key an erster Stelle stehen." • Ergänzung: „In der [TR-03130] Teil 1 ist festgelegt, dass der eID-Server zwei Pseudonyme von der Karte abruft, wenn im Berechtigungszertifikat zwei Sector Public Keys enthalten sind, d.h. die Steuerung der Erzeugung zweier Pseudonyme erfolgt über die Berechtigungs-CA." • Ergänzung: „Die Dauer, für die zwei Pseudonyme erzeugt werden, muss zwischen Diensteanbieter und (neuer) Berechtigungs-CA verabredet werden. Grundsätzlich ist auch eine dauerhafte Erzeugung des alten Pseudonyms denkbar (dann muss der Diensteanbieter seine Datenbank nicht migrieren). Es muss beachtet werden, dass solange der alte Sector Public Key im Zertifikat enthalten ist, keine anderen Migrationen (siehe Einleitung) möglich sind."
2.0	18.09.2015	Einarbeitung der externen Kommentare
2.0.1	24.09.2015	Korrektur Schreibfehler, Kapitel 1.4.4 Korrektur der Prüfung Link-Zertifikate, Anpassung Definition CVCA-Link-Zertifikate (Kapitel 8)
2.0.7	02.05.2016	Einfügen MDS-Zertifikate 1. Entwurf
2.0.7.1	30.08.2016	Einfügen MDS-Zertifikate final
2.1	10.10.2016	Bereinigung von Kapitel 6 Sicherheitsmaßnahmen für Schlüsselpaare inkl. Verweis auf das Dokument „Key Lifecycle Security Requirements" Version 1.0
2.1.1	01.12.2016	Anpassung der Kapitelstruktur zur besseren Übersicht bzgl. MDS-Zertifikate; Ergänzung Vorgaben für die Form der MDS Zertifikatsanträge.
2.2 - Draft	12.07.2017	Anpassung an Änderungen des Personalausweisgesetzes [PAuswG]. Erweiterung der Zertifikatsbeantragung.
2.2 - Draft 2	27.09.2017	Einarbeitung der Kommentare zu Version 2.2
2.2	24.10.2017	Finalisierung der Version 2.2
2.3 - Draft	03.06.2019	Anpassungen für Zwecke der Qualitätssicherung gemäß §36 Abs. 1 S. 2 [PAuswV]

Version	Datum	Beschreibung
2.3	28.06.2019	Finalisierung der Version 2.3
2.4	22.07.2021	Ergänzungen und Anpassungen zur Einführung des Ummelde-/Schreibdiensts und PIN-Rücksetzdiensts.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die Country Verifying Certification Authority eID-Anwendung (CVCA-eID) ist die Wurzelzertifizierungsinstanz für die Zertifikate zur Berechtigung für den Zugriff auf die eID-Anwendung der hoheitlichen Dokumente Personalausweis oder elektronischer Aufenthaltstitel, sowie der Online-Ausweisfunktion der eID-Karte für Unionsbürger oder der Smart-eID.

In dieser Certificate Policy (CP) werden die Regeln der CVCA-eID Public Key Infrastruktur (CVCA-eID PKI) und die Pflichten ihrer Teilnehmer festgelegt.

Die Vorgaben für die Vergabe von Berechtigungszertifikaten an Anbieter des öffentlichen Sektors anderer EU-Mitgliedsstaaten im Kontext der eIDAS-Verordnung [eIDAS-VO] sind in [CP-Annex] festgelegt.

Die Certificate Policy ist in der Personalausweisverordnung ([PAuswV]) gemäß §32 als rechtlich bindend verankert.

Inhaltliche Grundlagen der CVCA-eID PKI finden sich in den folgenden Dokumenten:

- Technische Richtlinie „eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control – Personalausweis, elektronischer Aufenthaltstitel und eID-Karte für Unionsbürger“ - [TR-03127],
- Technische Richtlinie „Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS-Token“- [TR-03110],
- Gesetz über den Personalausweis und den elektronischen Identitätsnachweis (Personalausweisgesetz) – [PAuswG],
- Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (Aufenthaltsgesetz) – [AufenthG],
- Verordnung über Personalausweise, eID-Karten für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis – [PAuswV],
- Aufenthaltsverordnung – [AufenthV],
- Technische Richtlinie „PKI for the Extended Access Control (EAC), Protocols for the Management of Certificates and CRLs” - [TR-03129]

1.1 Definitionen

Der Begriff **eID-Dokument** wird im vorliegenden Dokument als Oberbegriff für den Personalausweis, den elektronischen Aufenthaltstitel, die eID-Karte für Unionsbürger bzw. deren Online-Ausweisfunktion sowie für die Smart-eID verwendet.

Die in diesem Dokument in Großbuchstaben verwendeten Schlüsselworte sind auf Basis der folgenden Übersetzungstabelle gemäß [RFC2119] zu interpretieren:

Deutsch	Englisch
MUSS / MÜSSEN	MUST
DARF KEIN(EN) / DÜRFEN KEIN(EN) / DARF NICHT / DÜRFEN NICHT	MUST NOT
VORAUSGESETZT	REQUIRED
SOLL / SOLLEN	SHALL
SOLL NICHT / SOLLEN NICHT	SHALL NOT
SOLLTE / SOLLTEN	SHOULD
SOLLTE NICHT / SOLLTEN NICHT	SHOULD NOT
EMPFOHLEN	RECOMMENDED
KANN / KÖNNEN / DARF / DÜRFEN	MAY
OPTIONAL	OPTIONAL

Tabelle 1: Übersetzungstabelle RFC 2119

1.2 Überblick

Die **CVCA-eID PKI** ist gemäß [TR-03110] in eine drei-stufige Hierarchie gegliedert, bestehend aus CVCA-eID-, DV- und Terminal-Ebene.

Die Wurzelinstanz bildet die CVCA-eID, welche entsprechend §32 [PAuswV] durch das Bundesamt für Sicherheit in der Informationstechnik betrieben wird.

Die CVCA-eID gibt zwei Arten von Zertifikaten heraus:

- zum einen Card Verifiable Zertifikate (CV-Zertifikate), welche für die Terminal-Authentisierung gemäß [TR-03110] verwendet werden,
- zum anderen Metadaten Signer Zertifikate (MDS-Zertifikate), welche die Nutzung von eIDAS-Anwendungen gemäß eIDAS-Verordnung [eIDAS-VO] (siehe Kapitel 1.2.2) unterstützen.

Das jeweils aktuelle CV-Zertifikat der CVCA-eID wird bei der Produktion der eID-Dokumente als Vertrauensanker in den Chip eingebracht.

Die **Document Verifier (DV)** werden in hoheitliche DV und nicht-hoheitliche DV unterteilt:

- **Hoheitliche DV** werden gemäß §36 (2) [PAuswV] durch das Bundesministerium des Innern bestimmt und stellen Zertifikate für die zur Identitätsfeststellung berechtigen Behörden (Ausweis- und Kontrollbehörden) (vgl. §36 (1) [PAuswV]) für die folgenden Nutzungsszenarien aus:
  - Qualitätssicherung bei der Ausgabe der eID-Dokumente bzw. anhand von Testausweisen
  - Auskunftsbegehren des Ausweisinhabers
  - Änderungen der Daten der eID-Funktion im eID-Dokument
  - PIN-Rücksetzdienst

- **Nicht-hoheitliche DV** erstellen Berechtigungszertifikate für den elektronischen Identitätsnachweis gemäß §18 [PAuswG] und das Vor-Ort-Auslesen gemäß §18a [PAuswG] in den Bereichen eBusiness und eGovernment und werden auch als Berechtigungszertifikateanbieter (BerCAs) bezeichnet.

Die dritte Ebene der CVCA-eID PKI bilden die **Terminals.** Auch hier wird zwischen hoheitlichen und nicht-hoheitlichen Terminals unterschieden:

- **Hoheitliche Terminals** kommen in verschiedenen Anwendungsbereichen zum Einsatz.
  - Hoheitliche Terminals die Berechtigungszertifikate von zur Identitätsfeststellung berechtigten Behörden verwenden. Gemäß §36 (2) [PAuswV] legt das Bundesministerium des Innern fest, welche Behörden dies sind. Neben den Kontrollbehörden zählen auch die Melde-, Ausweis- und

Ausländerbehörden zu dieser Gruppe. Letztere ermöglichen dem Ausweisinhaber gemäß [PAuswV] bzw. [AufenthV], sich die elektronischen Daten seines eID Dokuments, mit Ausnahme der Smart-eID, anzeigen oder bestimmte Datengruppen ändern zu lassen.

- Gemäß §36 (1) 2 [PAuswV] dürfen hoheitliche Berechtigungszertifikate zum Zwecke der Qualitätssicherung anhand von Testausweisen an das Bundesamt für Sicherheit in der Informationstechnik ausgegeben werden.
- Hoheitliche Terminals für die Online-Dienste PIN-Rücksetzdienst und Ummelde-/Schreibdienst. Diese werden im folgenden als hoheitliche Online-Dienste bezeichnet.

- **Nicht-hoheitliche Terminals** verwenden Berechtigungszertifikate von Diensteanbietern. Hierbei wird entsprechend den verschiedenen Anwendungsfällen zwischen folgenden Typen unterschieden:
  - **Nicht-hoheitliche Terminals für den elektronischen Identitätsnachweis** verwenden Berechtigungszertifikate von Typen von Diensteanbietern für den elektronischen Identitätsnachweis nach §18 [PAuswG]:
    - Diensteanbietern nach §21 [PAuswG] für den elektronischen Identitätsnachweis, oder
    - Identifizierungsdiensteanbieter nach §21b [PAuswG] für den elektronischen Identitätsnachweis.
  - **Nicht-hoheitliche Terminals für das Vor-Ort-Auslesen** verwenden Berechtigungszertifikate von Vor-Ort-Diensteanbieter §21a [PAuswG] für das Vor-Ort-Auslesen nach §18a [PAuswG].

  Diensteanbieter und Identifizierungsdiensteanbieter für den elektronischen Identitätsnachweis als auch Vor-Ort-Diensteanbieter müssen bei der Vergabestelle für Berechtigungszertifikate (VfB) zum Erhalt von Berechtigungen registriert sein, erhalten aber ihre digitalen Berechtigungszertifikate von einer BerCA. Die Erteilung von Berechtigungen, dass eine BerCA einen Zertifikatsnehmer registrieren darf, obliegt gemäß [PAuswG] der VfB. Diese legt auch die Bedingungen für die Aufrechterhaltung bzw. Sperrung der Registrierungen fest und überwacht deren Einhaltung. Die Kommunikation zwischen den PKI-Instanzen findet nach der Registrierung primär über Kommunikationsschnittstellen gemäß [TR-03129] statt.

Sofern nicht explizit anders erwähnt, wird der Begriff „Diensteanbieter“ im Folgenden i.A. so verwendet, dass er sowohl Diensteanbieter und Identifizierungsdiensteanbieter für den elektronischen Identitätsnachweis als auch Vor-Ort-Diensteanbieter umfasst.

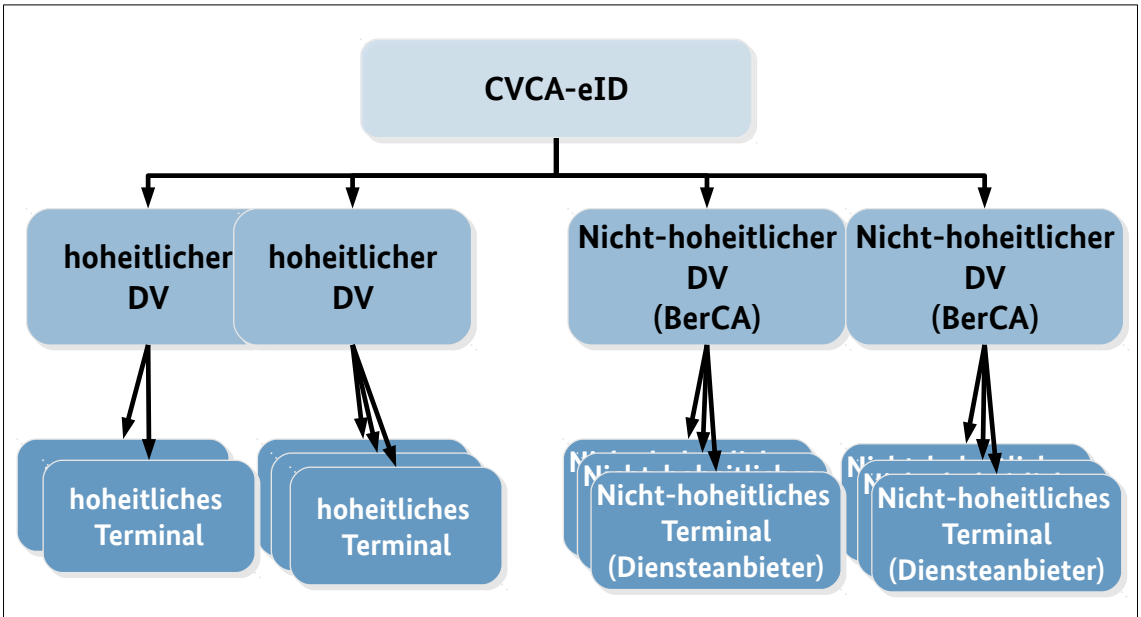

Abbildung 1: Aufbau der CVCA-eID PKI

1.2.1 Technische Ausprägungen von Terminals

Es kann verschiedene technische Ausprägungen von Terminals geben:

- **integrierte Terminals:** Diese Geräte verfügen über einen integrierten Terminal-Schlüssel und die zugehörige vollständige EAC-Zertifikatskette und können somit selbstständig die eID-Authentisierung mit einem eID-Dokument durchführen. Zu den integrierten Terminals gehören:
  - EAC-Boxen nach [TR-03131]
  - Offline Terminals (z.B. Automaten)
- **verteilte Terminals:** Bei verteilten Terminals wird der Speicher des privaten Schlüssels des Berechtigungszertifikats in einem anderen System als die Schnittstelle des Terminals zum eID-Dokument realisiert. Sie sind i.d.R. als Online-Terminals über das Internet erreichbar und jeweils in ein Remote Terminal und ein Lokales Terminal unterteilt.

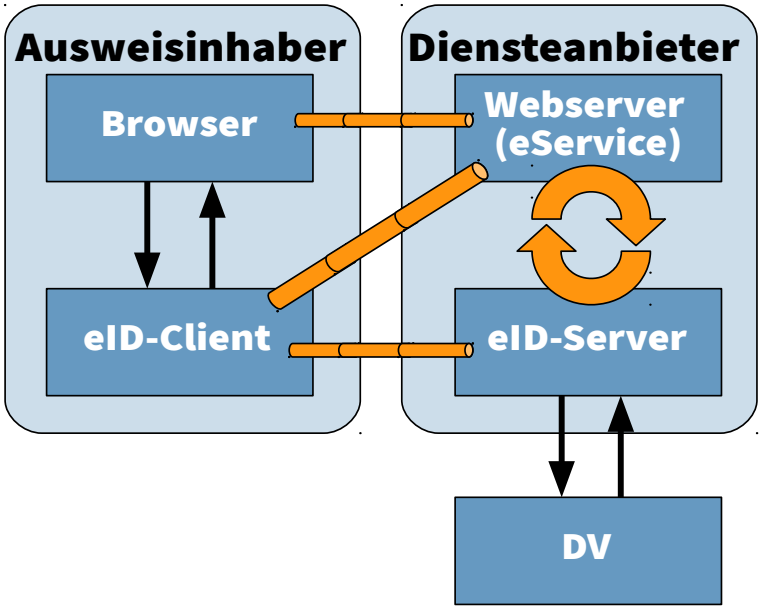

Abbildung 2: Verteiltes Terminal

Das **Remote Terminal** befindet sich im Einflussbereich des Diensteanbieters und besteht aus eService und eID-Server (siehe [TR-03130] Teil1). Letzterer muss nach den Vorgaben aus [TR-03130], Teil 2, betrieben werden. Es hat die Berechtigung zum Zugriff auf Daten der Online-Ausweisfunktion der eID-Dokumente, d.h. es besitzt den privaten Schlüssel des Terminal-Zertifikats (genauer der eID-Server). Das Remote Terminal schickt dem Lokalen Terminal die Zertifikatskette des Terminal-Zertifikats und die vom Chip des eID-Dokuments angeforderte Signatur einer Challenge. Die Signatur wird mit dem privaten Schlüssel des Terminals erzeugt.

Das **Lokale Terminal** befindet sich im Einflussbereich des Ausweisinhabers und besteht aus dem eID-Client (siehe [TR-03124-1]) und dem User Agent (z.B. Internet-Browser). Es interagiert mit dem Nutzer, dem eID-Dokument, und dem Remote Terminal, aber es ist nicht berechtigt, auf die Daten der eID-Anwendung zuzugreifen. Die vom Remote Terminal gesendete Kette der Zertifikate für die Terminalauthentisierung wird dem Ausweisinhaber angezeigt. Nur wenn der Nutzer zustimmt, leitet das Lokale Terminal die Zertifikate an den Chip des eID-Dokuments weiter. Zusätzlich prüft der eID-Client, ob die aufgerufene Website des eService mit den Angaben zum eService im Terminal-Zertifikat übereinstimmt.

1.2.2 Metadaten Signer Zertifikate

Zur Ermöglichung der Nutzung von eIDAS-Anwendungen gemäß eIDAS-Verordnung (siehe [eIDAS-VO]) werden entsprechend der [eIDAS-Inter] so genannte eIDAS-Konnektoren eingesetzt.

Für diesen Zweck werden in der CVCA-eID PKI zusätzlich MDS-Zertifikate ausgestellt. Die MDS-Zertifikate werden außer von der CVCA-eID nur von den nicht-hoheitlichen Instanzen für den elektronischen Identitätsnachweis der CVCA-eID PKI beantragt oder ausgestellt.

Die CVCA-eID stellt, zusätzlich zum CVCA Zertifikat und den DV-Zertifikaten, ein selbst-signiertes Metadaten Signer Root-Zertifikat sowie Metadaten Signer SubCA-Zertifikate für die Document Verifier aus.

Ein DV stellt für jeden bei ihm registrierten Diensteanbieter ein Metadaten Signer DA-Zertifikat aus, sofern der DA eIDAS-Anwendungen anbieten möchte. Erzeugung, Besitz und Nutzung der entsprechenden privaten Schlüssel erfolgt analog zu den privaten Schlüsseln der Terminal-Zertifikate[1]. Die signierten Metadaten werden dann vom DA unter einer öffentlichen URL zur Verfügung gestellt. Der Rückruf von Metadaten Signer Zertifikaten erfolgt DA-spezifisch. Im Sinne der [eIDAS-Inter] ist der Diensteanbieter der Konnektor.

1 d.h. wenn der Diensteanbieter den Betrieb des eID-Servers extern beauftragt, dann erzeugt und nutzt dieser den Schlüssel im Auftrag des DA. Ein eID-Server Betreiber kann somit unterschiedliche Schlüsselpaare für unterschiedliche DA verwalten.

Die MDS-Zertifikate entsprechen dem X.509 Format gemäß [RFC5280] und werden nach den folgenden Zertifikatstypen unterschieden:

- **Metadaten Signer Root-Zertifikat**, mit dem zugehörigen privaten Schlüssel werden die Metadaten Signer SubCA-Zertifikate signiert. Das Metadaten Signer Root-Zertifikat wird von der CVCA-eID ausgestellt und auf deren Website veröffentlicht. Außerdem stellt die CVCA-eID die Metadaten Signer SubCA-Zertifikate für die Document Verifier aus.
- **Metadaten Signer SubCA-Zertifikat**, mit dem zugehörigen privaten Schlüssel werden die Metadaten Signer Zertifikate signiert. Die Metadaten Signer Zertifikate werden von den DV ausgestellt.
- **Metadaten Signer DA-Zertifikat**, mit dem zugehörigen privaten Schlüssel werden die Metadaten signiert. Es wird für jeden Diensteanbieter ein eigenes Metadaten Signer DA-Zertifikat ausgestellt.
- **Metadaten**, diese werden vom jeweiligen Diensteanbieter gemäß [eIDAS-Inter] ausgestellt und mit dem privaten Schlüssel des zugehörigen Metadaten Signer DA-Zertifikats signiert.

Zusätzlich werden in den Metadaten TLS-Zertifikate für die Diensteanbieter hinterlegt. Alle oben genannten Zertifikate MÜSSEN den Anforderungen aus [eIDAS-Crypto] und der [TR-03116-2] entsprechen.

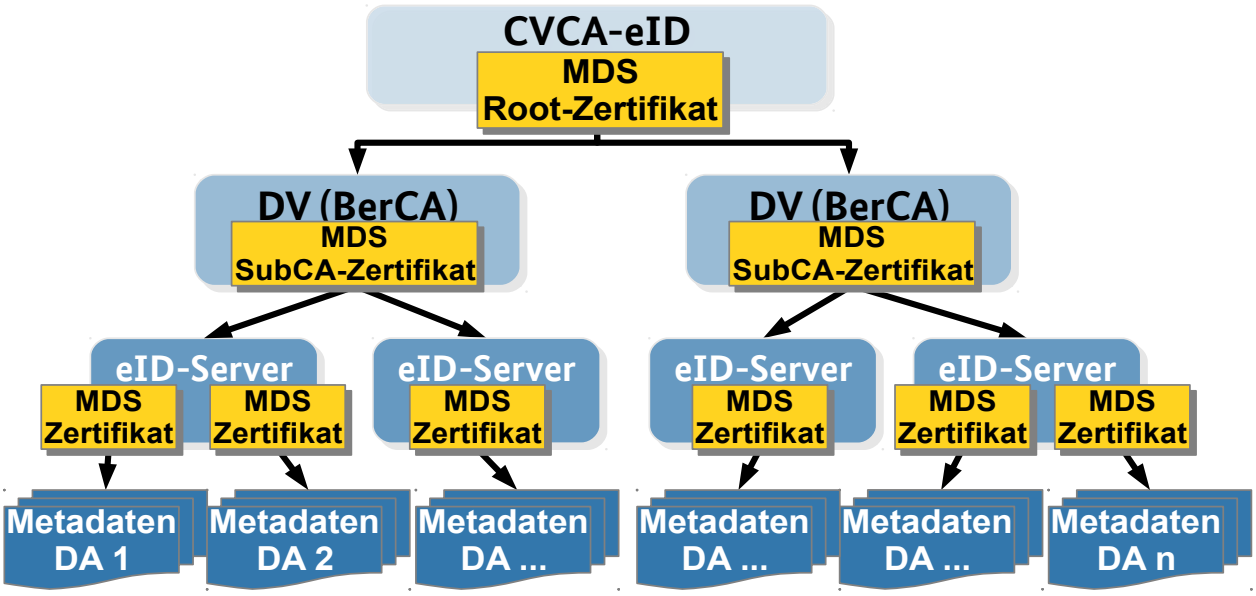

Abbildung 3: Erweiterung der CVCA-eID PKI um die Metadaten Signer Zertifikate

1.3 Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) der deutschen Country Verifying Certification Authority - electronic Identity (CVCA-eID) und wird wie folgt identifiziert:

- **Titel:** Certificate Policy für die Country Verifying Certification Authority eID-Anwendung (CP CV-CA-eID)
- **Version:** 2.4 vom 22. Juli 2021
- **OID:** `0.4.0.127.0.7.3.1.1.2.2`

Das Dokument kann unter https://www.bsi.bund.de/cvca-eID bezogen werden.

1.4 Teilnehmer der PKI

In diesem Unterkapitel werden die Teilnehmer (Zertifizierungsinstanzen, Registrierungsinstanzen, Zertifikatsnehmer und Zertifikatsnutzer) der CVCA-eID PKI aufgeführt. Die nachfolgende Tabelle zeigt einen Überblick über die Teilnehmer der PKI:

Instanz der PKI	Zertifizierungs-instanz	Registrierungsin-stanz	Zertifikatsnehmer	Zertifikatsnutzer
CVCA-eID	■	■	■	■
DV	■	■	■	■
Terminal			■	■
eID-Dokument				■
eIDAS-Services gemäß [eIDAS-Inter]				■

Tabelle 2: Übersicht der PKI-Teilnehmer

1.4.1 Zertifizierungsinstanzen

Eine Zertifizierungsinstanz ist für die Ausstellung von Zertifikaten zuständig und wird auch als Zertifikatsgeber oder Zertifikatsaussteller bezeichnet.

Aufgaben der Zertifizierungsinstanz (Certification Authority, CA) sind:

- das sichere Erzeugen und Verwalten von Schlüsselpaaren;
- das Prüfen von Zertifikatsanträgen auf Korrektheit gemäß CP und auf Rechtmäßigkeit bzgl. der Statusinformationen der Registrierungsinstanz über den Antragsteller;
- das Signieren von Zertifikatsanträgen;

Die Kommunikation zwischen Zertifizierungs- und Registrierungsinstanz muss durch angemessene Maßnahmen abgesichert werden.

1.4.2 Registrierungsinstanzen

Eine Registrierungsinstanz ist für die Registrierung und Verwaltung der Zertifikatsnehmer zuständig.

Die Aufgaben der Registrierungsinstanz (Registration Authority, RA) sind:

- Prüfung der Registrierungsunterlagen;
- Durchführen der zweifelsfreien Identifizierung und Authentifizierung des Antragstellers;
- Durchführen der Registrierung;

- Speicherung der Registrierungsinformationen und des Status der zugehörigen Registrierung;
- Aktualisieren von Registrierungsinformationen;
- Sperrung von Zertifikatsnehmern bei Sicherheitsvorfällen oder Nicht-Erfüllung von Registrierungsbedingungen;
- Sperrung von MDS-Zertifikaten bei Sicherheitsvorfällen oder Nicht-Erfüllung von Registrierungsbedingungen;
- Entgegennehmen von Sperranträgen bzw. Informationen, die zur Sperrung eines Zertifikatsnehmers führen können;
- Entsperrung von Zertifikatsnehmern;
- Entgegennehmen und Prüfen von Zertifikatsanträgen;
- Weiterleiten von Zertifikatsanträgen und Statusinformationen über die Zertifikatsnehmer an die Zertifizierungsinstanz;

Bei den nicht-hoheitlichen Document Verifiern übernimmt die VfB einen Teil der organisatorischen Aufgaben der RA, die Registrierung und Sperrung betreffen[2]. Um die Entscheidungen der VfB ordnungsgemäß durchsetzen zu können, müssen die BerCAs jedoch zusätzlich eine Registrierungsinstanz betreiben, welche die Angaben der VfB technisch umsetzt. Die Einzelheiten bezüglich der Aufgabenabgrenzung im Bereich RA zwischen BerCA und VfB regelt die VfB.

1.4.3 Zertifikatsnehmer

Ein Zertifikatsnehmer ist der Inhaber eines Zertifikats und im Besitz des zugehörigen privaten Schlüssels. Die Inhaberschaft des Zertifikats kann eindeutig über den Namen im Zertifikat und den Namen des Ausstellers des Zertifikats zugeordnet werden.

Der Zertifikatsnehmer ist für die rechtzeitige Erstellung von Zertifikatsanträgen zuständig, wenn er ein Folgezertifikat beantragen möchte.

Zertifikatsnehmer können sein:

- CVCA-eID, stellt sich als Vertrauensanker der PKI selbst-signierte CVCA-Zertifikate sowie CVCA-Link-Zertifikate aus; des Weiteren stellt sich die CVCA-eID selbst-signierte Metadaten Signer Root-Zertifikate sowie die zugehörigen MDS Root Link-Zertifikate aus;
- Document Verifier erhalten DV-Zertifikate sowie MDS SubCA-Zertifikate von der CVCA-eID;
- Terminals erhalten Terminal-Zertifikate von den Document Verifiern. Diese Zertifikate werden auch Berechtigungszertifikate genannt. Des Weiteren können Terminals Metadaten Signer DA-Zertifikate von den DVs erhalten.

1.4.4 Zertifikatsnutzer

Zertifikatsnutzer verwenden die Zertifikate der CVCA-eID PKI, um Berechtigungen festzustellen und Signaturen zu prüfen.

Zertifikatsnutzer sind unter anderen:

- Die CVCA-eID, sie prüft die Signaturen der Wiederholungsanträge für CV-Zertifikate der DV;
- Document Verifier, sie prüfen die Signaturen
  - der Wiederholungsanträge der Diensteanbieter,
  - der CVCA-eID auf den DV-Zertifikaten und den CVCA Zertifikaten und
  - CVCA Link-Zertifikaten,
  - den MDS Root-Zertifikaten,
  - den MDS Link-Zertifikaten und
  - den MDS SubCA-Zertifikaten;

2 Siehe auch Kapitel 3.2.3 „Registrierung von Terminals“

- Terminals, sie prüfen die Signaturen auf den DV-Zertifikaten und den CVCA Zertifikaten bzw. CVCA Link-Zertifikaten;
- hoheitliche eID-Dokumente, sie prüfen die Signaturen der Terminal-Zertifikate, der DV-Zertifikate und der CVCA Link-Zertifikate während der Terminalauthentisierung gemäß [TR-03110].
- eIDAS-Services gemäß [eIDAS-Inter], diese prüfen die Zertifikatsketten der Metadaten Signer Zertifikate sowie die Signaturen über die Metadaten.

1.4.5 Kommunikation zwischen den Teilnehmern

Die Beantragung und Versendung von Zertifikaten findet in der Regel über die Kommunikationsschnittstelle gemäß [TR-03129] statt, die jeder PKI-Teilnehmer einrichten MUSS, der Zertifikate beantragt und/oder ausstellt.

Jede Kommunikationsverbindung gemäß [TR-03129] MUSS über die bei der Registrierung hinterlegten Kommunikationszertifikate der Teilnehmer unter Verwendung von TLS authentisiert und verschlüsselt werden.

Sowohl für die verwendeten Kommunikationszertifikate als auch den Einsatz von TLS MÜSSEN die Vorgaben aus [TR-03116-4] eingehalten werden. Im Rahmen dieser Vorgaben gelten die folgenden Festlegungen:

- für die Identifizierung von Kommunikationspartnern SOLLTE die PKI-basierte Variante gewählt werden[3];
- für die Rückrufprüfung SOLLTE die Variante CRL Distribution Point gewählt werden[3];
- die CVCA-eID DARF als Wurzelzertifikat der Kommunikationszertifikate das CSCA-Zertifikat verwenden. In diesem Fall DARF die maximale Gültigkeitsdauer von 5 Jahren für CA-Zertifikate überschritten werden;
- CVCA und Document Verifier MÜSSEN für Kommunikationszertifikate sowohl die Verwendung RSA- als auch ECC-basierten Schlüssel ermöglichen .

Die Kommunikationsschnittstelle gemäß [TR-03129] auf Seiten der CVCA-eID wird auch als SPOC (Single Point of Contact) bezeichnet.

Jedwede weitere Kommunikation mit der **CVCA-eID** findet von Seiten der CVCA über die folgende E-Mail Adresse statt[4]:

cvca-eid@bsi.bund.de

Jeder **Document Verifier** MUSS ebenfalls ein Funktionspostfach für die Kommunikation mit der CVCA einrichten und dieses bei der Registrierung angeben. Auf dieses Funktionspostfach MÜSSEN alle relevanten Personen Zugriff haben. Die CVCA berücksichtigt keine E-Mail Adressen von Einzelpersonen[5].

Diese E-Mail-Adressen von CVCA und DV MÜSSEN als sekundäre Kommunikationsschnittstelle verwendet werden, wenn eine Kommunikation gemäß [TR-03129] nicht möglich ist.

Kommunikation (neben der Zertifikatsverteilung) zwischen **Document Verifiern und Terminals**, die nicht über die Schnittstellen gemäß [TR-03129] erfolgen kann, SOLLTE über Schnittstellen erfolgen, welche durch die VfB bzw. die Certificate Policies der Document Verifier festgelegt sind.

1.4.6 Sperrmerkmale

Mit Hilfe des Sperrmerkmals kann der Terminalbetreiber feststellen, ob das zur Authentisierung vorgelegte eID-Dokument gesperrt ist (vgl. [TR-03127]). Das Sperrmerkmal wird durch das eID-Dokument im Moment der Authentisierung aus dem Sector Public Key des Diensteanbieters (Bestandteil des Berechtigungszertifikates) und einem geheimen Schlüssel des eID-Dokuments gebildet.

3 In Einzelfällen kann bei der Kommunikation zwischen DV und Terminal hiervon nach Absprache mit der CVCA-eID abgewichen werden. Der abweichende Prozess MUSS in der CP des DV beschrieben werden.

4 In Einzelfällen kann hiervon nach Absprache mit der CVCA-eID abgewichen werden.

5 Sollte es aus organisatorischen Gründen notwendig sein, dass die einzelnen Mitarbeiter des DV als Absender der E-Mails fungieren, SOLLEN sie ihr eigenes Funktionspostfach in Kopie nehmen.

Ein hoheitlicher DV für die Ummelde- und PIN-Rücksetzdienste MUSS regelmäßig aktuelle dienstespezifische Sperrlisten erzeugen und für die bei ihnen registrierten Diensteanbieter bereitstellen. Die veraltete eID-Sperrliste MUSS gelöscht werden.

1.4.7 Pseudonyme[6]

Der Ausweis bietet die Möglichkeit der pseudonymen Authentisierung, d.h. der Ausweisinhaber kann sich gegenüber einem Diensteanbieter authentisieren, ohne persönliche Daten freizugeben. Insbesondere bildet der Ausweis für jeden Diensteanbieter ein anderes Pseudonym, so dass das Verbinden von Pseudonymen über Diensteanbietergrenzen hinweg nicht möglich ist (vgl. [TR-03127]).

Im Unterschied zu den Sperrmerkmalen werden Pseudonyme dauerhaft genutzt, d.h. sie werden (entsprechend der Berechtigung) vom Diensteanbieter gespeichert.

Das Pseudonym wird – analog zum Sperrmerkmal – aus dem im Berechtigungszertifikat zertifizierten Sector Public Key und einem geheimen Schlüssel des Ausweises gebildet. Der Sector Private Key wird hierfür nicht benötigt.

1.4.8 Request-Signer-Zertifikate

Die Beantragung von CV-Zertifikaten erfolgt über Zertifikatsrequests, deren Authentizität und Integrität vor der Ausstellung des jeweiligen CV-Zertifikats durch organisatorische oder technische Maßnahmen gemäß dieser Certificate Policy sichergestellt wird.

Request-Signer-Zertifikate sind selbst-signierte Zertifikate im X.509-Format nach [RFC5280], deren Schlüssel zur Authentisierung von Zertifikatsanträgen genutzt werden KÖNNEN. Die Unterstützung und Nutzung von Request-Signer-Zertifikaten ist OPTIONAL und erfolgt in Abstimmung zwischen CVCA oder DV und Zertifikatsnehmer. In diesem Fall MÜSSEN die Request-Signer-Zertifikate bei der Registrierung bei der CVCA bzw. dem DV hinterlegt werden.

Die Gültigkeitszeit eines Request-Signer-Zertifikats DARF 3 Jahre bzw. die von der VfB ausgestellte Berechtigung des Zertifikatsnehmers (Terminal-Ebene) aus dem zugehörigen VfB-Bescheid NICHT überschreiten. Die Domain-Parameter des öffentlichen Schlüssels eines verwendeten Request-Signer-Zertifikats müssen den Domain-Parametern des CVCA-Zertifikats [TR-03116-2] entsprechen.

1.5 Administration der Certificate Policies

1.5.1 CVCA-eID Policy

Verantwortlich für Erstellung, Pflege und Veröffentlichung dieser Certificate Policy ist das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die zuständigen Ansprechpartner für die Certificate Policy und die CVCA-eID können über die folgenden Angaben kontaktiert werden:

- **Organisation:** Bundesamt für Sicherheit in der Informationstechnik
- **Adresse:** Godesberger Allee 185-189, 53175 Bonn
- **E-Mail:** cvca-eID@bsi.bund.de
- **Webseite:** https://www.bsi.bund.de/cvca-eID

Jede aktualisierte Version der Certificate Policy wird den Anwendern unverzüglich über die Internetseite des BSI (https://www.bsi.bund.de/cvca-eID) zur Verfügung gestellt.

Weitere Dokumente der CVCA-eID wie z.B. Certificate Practice Statement (CPS), Sicherheitskonzept oder Betriebskonzept sind rein interne Dokumente, welche bei Audits herangezogen werden können. Diese Dokumente entsprechen den Anforderungen der CP CVCA-eID.

Folgende Informationen MÜSSEN durch die CVCA-eID auf der **BSI CVCA-eID Webseite** (https://www.bsi.bund.de/cvca-eID) veröffentlicht werden:

- die CVCA-eID PKI Certificate Policy

6 Pseudonym = dienste- und kartenspezifisches Merkmal gemäß §2 Abs. 5 [PAuswG]

- alle gültigen CVCA-Zertifikate

Die Technischen Richtlinien des BSI, auf die innerhalb dieses Dokumentes verwiesen wird, stehen unter https://www.bsi.bund.de/ElektronischeAusweiseTR zur Verfügung.

1.5.1.1 Änderungen an der CVCA-eID Policy

Erfolgen Änderungen an der CVCA-eID Policy, welche die Document Verifier oder die Terminalbetreiber betreffen, erhalten diese das neue Dokument spätestens 30 Tage vor Inkrafttreten zur Kenntnis.

Bei Änderungen, die direkte Auswirkung auf den Betrieb der DV bzw. der Terminals haben, wird eine Übergangsfrist in Relation zur Änderung in der neuen CVCA-eID Policy festgelegt. Mit Ende dieser Übergangsfrist ist die neue CVCA-eID Policy dann gemäß §32 [PAuswV] rechtlich bindend.

1.5.2 Certificate Policies der Document Verifier

Jeder Document Verifier MUSS eine eigene Certificate Policy erstellen. Die CP eines DV MUSS die folgenden Bedingungen erfüllen:

- alle Vorgaben aus der CVCA-eID CP für den DV und seine Zertifikatsnehmer MÜSSEN abgedeckt werden;
- die Vorgaben aus der CVCA-eID CP für den DV und seine Zertifikatsnehmer dürfen konkretisiert werden;
- Vorgaben für Zertifikatsnehmer SOLLTEN gegenüber der CVCA-eID CP ergänzt werden;
- die CP eines DV DARF den Vorgaben der CVCA-eID CP NICHT widersprechen oder diese in Hinblick auf Sicherheit oder Interoperabilität aufweichen;
- die CP eines DV MUSS der CVCA-eID zur Bestätigung der Erfüllung der o.g. Anforderungen vor Inkrafttreten vorgelegt werden;
- die CP eines DV MUSS veröffentlicht werden.

1.5.2.1 Änderungen an der DV CP

Bezüglich Änderungen der Certificate Policy von DV gelten die folgenden Regeln:

- bei einer neuen Version der CVCA-eID CP MUSS der DV seine Certificate Policy entsprechend anpassen; stellt der DV fest, dass die Änderungen der CVCA-eID CP keine inhaltlichen Auswirkungen auf die CP des DV haben, MÜSSEN zumindest Versionsnummer und Datum der CP des DV angepasst werden;
- wenn der DV seine CP ändert, MUSS er diese vor Veröffentlichung der CVCA-eID zur Bestätigung vorlegen[7];
- sind die beim DV registrierten Terminalbetreiber von der Änderung betroffen, MUSS der DV den Terminalbetreibern eine entsprechende Übergangsfrist zur Umsetzung der neuen Anforderungen gewähren.

7 Um diesen Prozess zu verkürzen, wird EMPFOHLEN, die CP mit Änderungsmarkierungen gegenüber der Vorgängerversion und einer Eigenerklärung, dass die Änderungen vollständig als solche gekennzeichnet sind, einzureichen.

2 Verzeichnisse und Bereitstellung von Zertifikaten

2.1 Zertifikatsverzeichnisse

Alle Zertifizierungsinstanzen und Zertifikatsnehmer der CVCA-eID PKI müssen ein Verzeichnis der eigenen sowie der von ihnen ausgestellten Zertifikate führen.

Die Verzeichnisse MÜSSEN jederzeit auf aktuellem Stand gehalten werden. Zudem MUSS der jeweilige PKI-Teilnehmer durch geeignete organisatorische und technische Maßnahmen sicherstellen, dass die Integrität der Informationen in seinen Verzeichnissen gewahrt bleibt.

Die zu speichernden Zertifikate sowie die einzuhaltenden Aufbewahrungszeiten für die Zertifikate sind in der folgenden Tabelle definiert:

Ebene	Zertifikatstyp	Archivierungsdauer
CVCA-eID	CVCA Zertifikate, CVCA Link-Zertifikate	Zertifikatslaufzeit[8] + 10 1/2 Jahre
	Alle ausgestellten DV Zertifikate	Zertifikatslaufzeit + 10 1/2 Jahre
DV	Alle eigenen DV Zertifikate	Zertifikatslaufzeit + 2 Jahre
	Alle ausgestellten Terminal Zertifikate	Zertifikatslaufzeit + 2 Jahre
Terminal	Alle eigenen Terminal Zertifikate	Zertifikatslaufzeit + 6 Monate
MDS Root-Zertifikat	Alle eigenen und ausgestellten MDS-Zertifikate sowie die ausgestellten CRLs	Zertifikatslaufzeit + 10 1/2 Jahre
MDS SubCA-Zertifikat	Alle eigenen und ausgestellten MDS-Zertifikate sowie die ausgestellten CRLs	Zertifikatslaufzeit + 2 Jahre
Metadaten Signer	Alle eigenen Metadaten Signer sowie die signierten Metadaten	Zertifikatslaufzeit + 2 Jahre

Tabelle 3: Archivierung öffentlicher Schlüssel

2.2 Bereitstellung von Zertifikaten

CVCA-eID

Die CVCA-eID MUSS zu jeder Zeit alle für die eID-Authentisierung (siehe [TR-03110]) erforderlichen Zertifikate und Listen bereitstellen:

- CVCA Zertifikate
- CVCA Link-Zertifikate
- aktuelle Defectlist
- aktuelles CSCA Zertifikat.
- aktuelles Metadaten Signer Root-Zertifikat.

Die CVCA Zertifikate und die Defectlist können direkt über die Kommunikationsschnittstelle gemäß [TR-03129] abgerufen werden. Über diesen Zugang ist auch das CSCA Zertifikat in Form einer Masterlist (siehe [TR-03129]) verfügbar.

Das aktuelle Metadaten Signer Root-Zertifikat wird nach Ausstellung an die DV per E-Mail versendet.

8 Die Zertifikatslaufzeit entspricht dem Gültigkeitszeitraum des Zertifikats, beschrieben in Abschnitt 4.7 Gültigkeitszeiträume von Zertifikaten und Schlüsselpaaren.

Die aktuellen Root-Zertifikate (CVCA, CSCA und Metadaten Signer Root-Zertifikat) sind zusätzlich auf der Webseite des BSI verfügbar[9].

DV-Ebene

Ein Document Verifier MUSS dem Terminalbetreiber zu jeder Zeit alle für die eID-Authentisierung (siehe [TR-03110]) erforderlichen Zertifikate bereitstellen, dies erfolgt über die Kommunikationsschnittstelle gemäß [TR-03129].

Die erforderlichen Zertifikate sind:

- alle CVCA Zertifikate bzw. CVCA Link-Zertifikate, die innerhalb der letzten 10 1/2 Jahre gültig waren,
- das eigene derzeit gültige DV-Zertifikat,
- das Metadaten Signer Root-Zertifikat und das SubCA Zertifikat.

Ebenso MUSS der DV die aktuelle Defectlist und das aktuelle CSCA Zertifikat über die Kommunikationsschnittstelle gemäß [TR-03129] zur Verfügung stellen. Die zugehörige jeweils aktuelle Sperrliste (Certificate Revocation List, CRL) für die Passive Authentisierung gemäß [TR-03110] kann über den im CSCA Zertifikat angegebenen Sperrlisten-Verteilungspunkt (CRL Distribution Point, CRL DP) abgerufen werden.

2.3 Registrierungsverzeichnisse

Jede Registrierungsinstanz der CVCA-eID PKI MUSS ein Verzeichnis führen, welches die Kontaktdaten, Registrierungsinformationen und den Registrierungsstatus (Sperrinformationen) aller bei der Instanz registrierten PKI-Teilnehmer beinhaltet.

Dieses Verzeichnis MUSS gegen unbefugte Zugriffe und Veränderungen geschützt sein und immer auf dem aktuellen Stand gehalten werden.

Ein **Document Verifier** MUSS jederzeit in der Lage sein, Bestand und Status aller bei ihm registrierten Terminals festzustellen und der CVCA auf Anfrage hierüber Auskunft geben.

9 https://www.bsi.bund.de/cvca-eID bzw. https://www.bsi.bund.de/csca

3 Identifizierung und Registrierung

3.1 Namensgebung

3.1.1 Namensgebung CV-Zertifikate

Der Bezeichner eines Zertifikats befindet sich im Feld „Certificate Holder Reference“ und MUSS dem Profil in [TR-03110] entsprechen.

CVCA-Zertifikat

Das Feld „Certificate Holder Reference” MUSS aus den folgenden verketteten Elementen bestehen:

1. Ländercode: DE
2. Holder Mnemonic: CVCAeID
3. Seriennummer: <SN> , mit den folgenden Eigenschaften:
   - 3.1. Länge: 5 Zeichen
   - 3.2. Codierung: ISO/IEC 8859-1
   - 3.3. Inhalt: Aufsteigende Seriennummer (00001 bis 99999), bei Überlauf Neubeginn bei 00001

DV-Zertifikat

Das Feld „Certificate Holder Reference” MUSS aus den folgenden verketteten Elementen bestehen:

1. Ländercode: DE
2. Holder Mnemonic: DVeID<Betreiberkürzel>
   - 2.1. <Betreiberkürzel>, mit den folgenden Eigenschaften:
     - 2.1.1. Länge: 2-4 Zeichen
     - 2.1.2. Codierung: ISO/IEC 8859-1
     - 2.1.3. Inhalt: Kürzel für den Namen des DV Betreibers
3. Seriennummer: <SN>, mit den folgenden Eigenschaften:
   - 3.1. Länge: 5 Zeichen
   - 3.2. Codierung: ISO/IEC 8859-1
   - 3.3. Inhalt: Aufsteigende Seriennummer (00001 bis 99999), bei Überlauf Neubeginn bei 00001

Der „Holder Mnemonic“ MUSS den Betreiber des DVs innerhalb der CVCA-eID PKI eindeutig identifizieren. Über die Vergabe des Kürzels entscheidet im Zweifelsfall die Registrierungsinstanz.

Der CHR eines DV-Zertifikats MUSS bezüglich des zugehörigen CVCA-Zertifikats eindeutig sein.

Terminal-Zertifikat

Ein Terminal-Zertifikat MUSS immer innerhalb der CVCA-eID PKI eindeutig über die Kombination der Werte der beiden folgenden Zertifikatsfelder identifizierbar sein (siehe [TR-03110]):

- Certification Authority Reference (CAR): Der Wert des CAR-Feldes MUSS dem des CHR-Feldes aus dem DV-Zertifikat des DVs entsprechen, welcher das Terminal-Zertifikat signiert.
- Certificate Holder Reference (CHR): Der Inhalt des CHR-Feldes wird vom ausstellenden DV unter Berücksichtigung der Anforderungen aus [TR-03110] vorgegeben.

Der CHR eines Terminal-Zertifikats MUSS bezüglich des zugehörigen DV-Zertifikats eindeutig sein.

3.1.1.1 Namensgebung von Request-Signer-Zertifikaten

Das Request-Signer-Zertifikat MUSS den Eintrag unter „Subject“ (siehe [RFC5280], Kapitel 4.1.2.6.) mit folgenden Datenfeldern enthalten:

1. „Organisational Unit“: Request Signer Certificate

2. „Common Name“: <Ländercode><HolderMnemonic><Seriennummer>, mit folgenden Eigenschaften
   2.1. Ländercode aus CV-Zertifikat des Zertifikatsnehmers
   2.2. Holder Mnemonic aus dem CV-Zertifikat des Zertifikatsnehmers
   2.3. Alphanumerische Seriennummer der Form: RSC<SN> mit fortlaufendem SN, so dass der Nummernraum der Seriennummer sich nicht mit der Seriennummern der CV-Zertifikate überschneidet.

Bei der Verwendung des Request-Signer-Zertifikats zur Beantragung von CV-Zertifikaten MUSS der Inhalt des Feldes „Common Name“ vom Zertifikatsnehmer in ISO/IEC 8859-1 konvertiert werden und zur Identifikation des Schlüssels der äußeren Signatur in dem entsprechenden Feld „Certificate Authority Reference“ des Antrags angegeben werden.

3.1.2 Namensgebung MDS-Zertifikate

In den X.509 MDS-Zertifikaten MUSS der Eintrag unter „Subject“ (siehe [RFC5280], Kapitel 4.1.2.6.) den Zertifikatsinhaber eindeutig in Bezug auf den „Subject“ der ausstellenden Instanz identifizieren.

Des Weiteren MUSS der Eintrag „Subject“ (siehe [RFC5280], Kapitel 4.1.2.4.) aus den folgenden Werten bestehen:

MDS Root-Zertifikat

1. „Country“: DE
2. „Organisation“: bund
3. „Organisational Unit“: bsi
4. „Common Name“: DECVCAeID Metadata Signer Root Germany
   4.1. Ländercode „DE“
   4.2. Holder Mnemonic aus dem CV-Zertifikat des Zertifikatsinhabers
   4.3. „Metadata Signer Root Germany“

MDS SubCA-Zertifikat

1. „Country“: DE
2. „Organisation“: <Name des DV Betreibers>
3. „Organisational Unit“: Metadata Signer SubCA Germany
4. „Common Name“: DEDVeID<Betreiberkürzel>
   4.1. Ländercode „DE“
   4.2. Holder Mnemonic aus dem CV-Zertifikat des Zertifikatsinhabers

MDS DA-Zertifikate

1. „Country“: DE
2. „Organisation“: <Name des Diensteanbieters>
3. „Organisational Unit“: Metadata Signer DA Certificate Germany
4. „Common Name“: DE<Holder Mnemonic des Diensteanbieters>

3.2 Registrierung

Jeder Zertifikatsnehmer MUSS seiner Zertifizierungsinstanz umgehend mitteilen, wenn sich Änderungen bzgl. seiner Registrierungsinformationen ergeben.

Jede Zertifizierungsinstanz bzw. Registrierungsinstanz MUSS eine Kommunikationsschnittstelle vorhalten, über welche die Zertifikatsnehmer Änderungen an ihren Registrierungsinformationen melden können. Die Registrierungsinstanz MUSS die Änderung der Registrierungsinformationen innerhalb von 72 Stunden in die entsprechende Registrierung einpflegen.

Nicht-hoheitliche DV MÜSSEN zusätzlich Meldungen von der VfB über Zertifikatsnehmer entgegennehmen und entsprechend verarbeiten.

Welche Institutionen als DV[10] von der CVCA-eID und welche Institutionen als nicht-hoheitliche Terminalbetreiber von der VfB oder als hoheitliche Terminalbetreiber von hoheitlichen DV registriert werden, wird durch die folgenden Rechtsvorschriften festgelegt:

- [PAuswG],
- [AufenthG],
- [PAuswV],
- [AufenthV].

3.2.1 Vorarbeiten zur Registrierung von DV

Im Vorfeld der Registrierung müssen die folgenden Arbeiten erfolgen:

1. **Alle DV:** Der DV MUSS die eigene DV Certificate Policy mit der CVCA-eID abstimmen (siehe Kapitel 1.5.2, Certificate Policies der Document Verifier);
2. **Alle DV:** Der DV MUSS den gewünschten Holder Mnemonic mit der CVCA-eID abstimmen (siehe Kapitel 3.1, Namensgebung);
3. Gesetzliche Anforderungen:
   3.1. **Nicht-hoheitliche DV:** Der DV MUSS die Anforderungen von §31 [PAuswV][11] erfüllen;
   3.2. **Hoheitliche DV:** Der DV MUSS die Anforderungen von §36 [PAuswV] erfüllen;
4. **Alle DV:** Der DV MUSS die folgenden Tests erfolgreich durchführen:
   4.1. Einreichen eines korrekten initialen Zertifikatsrequests des DV beim Test-System der CVCA-eID;
   4.2. Empfang des initialen DV-Zertifikats aus dem Test-System der CVCA-eID;
   4.3. Einreichen eines korrekten Wiederholungsantrags über die Kommunikationsschnittstelle gemäß [TR-03129] beim Test-System der CVCA-eID;
   4.4. Empfang des Folgezertifikats aus dem Test-System der CVCA-eID über die Kommunikationsschnittstelle gemäß [TR-03129];
5. **Alle DV:** Die o.g. und alle weiteren Tests MÜSSEN unter den folgenden Bedingungen durchgeführt werden:
   5.1. Das vom DV für die Tests verwendete IT-System MUSS dem später eingesetzten Wirk-System entsprechen (d.h. gleiche Software, Netzanbindung an das Internet)
   5.2. Der Holder Mnemonic für den Testbetrieb MUSS im Allgemeinen dem für den Wirkbetrieb vereinbarten Holder Mnemonic entsprechen, wobei der Abschnitt „DVeID“ durch „DVtID“ ersetzt werden MUSS;
   5.3. Die Schlüsselpaare der im Test-System verwendeten Zertifikatsanträge und TLS-Zertifikate MÜSSEN speziell für den Testbetrieb erzeugt werden und DÜRFEN NICHT in den Wirkbetrieb überführt werden;

3.2.2 Registrierung von DV

Zur Registrierung eines Document Verifiers bei der CVCA-eID MUSS ein bevollmächtigter Vertreter des Betreibers persönlich bei der CVCA-eID RA erscheinen.

3.2.2.1 Notwendige Unterlagen und Daten für die Registrierung

1. Antrag der den DV betreibenden Organisation auf Registrierung bei der CVCA-eID;

10 Im Gesetzestext werden die DV als Berechtigungszertifikateanbieter bzw. hoheitliche Berechtigungszertifikateanbieter bezeichnet.

11 Der Verweis auf einzelne Paragraphen der Gesetze oder Verordnungen ersetzt nicht die grundsätzliche Notwendigkeit die Gesetze und Verordnungen im Ganzen zu befolgen.

2. Kontaktdaten der Ansprechpartner des DV;
3. Funktionspostfach des DV;
4. Vertretungsvollmacht für den bevollmächtigten Vertreter sowie ein gültiger amtlicher Lichtbildausweis des Vertreters;
5. Informationen zum Typ des DV;
6. Gesetzliche Anforderungen:
   6.1. **Nicht-hoheitliche DV:** Nachweis der Erfüllung der Anforderungen von §31 [PAuswV];
   6.2. **Hoheitliche DV:** Nachweis der Erfüllung der Anforderungen von §36 [PAuswV];
7. die mit der CVCA-eID abgestimmte Certificate Policy des DVs (siehe Kapitel 1.5.2, „Certificate Policies der Document Verifier“);
8. Eigenerklärung zur Einhaltung der CP CVCA-eID und der eigenen CP DV;
9. Nachweis der Erfüllung der Anforderungen aus Kapitel 7, „Audits“;
10. die für die Kommunikation gemäß [TR-03129] benötigten Daten (siehe Kapitel 1.4.5, „Kommunikation zwischen den Teilnehmern“) inklusive der Fingerprints der hierfür benötigten TLS-Zertifikate, letztere in gedruckter Form;
11. initialer Zertifikatsrequest (siehe Kapitel 4.2.1 „Initiale Zertifikatsanträge für CV-Zertifikate“) oder alternativ in Abstimmung zwischen CVCA und DV ein Request-Signer-Zertifikat für die Authentisierung von Zertifikatsanträgen;
12. Fingerprint des initialen Zertifikatsrequests oder alternativ in Abstimmung zwischen CVCA und DV des Request-Signer-Zertifikats in gedruckter Form ;
13. **Nicht-hoheitliche DV:** initialer Zertifikatsrequest des MDS SubCA-Zertifikats sowie der zugehörige Fingerprint.

Sollte ein privatwirtschaftlicher Dienstleister für den Betrieb eines **hoheitlichen Document Verifiers beauftragt** werden, MUSS zusätzlich zu den genannten Unterlagen eine schriftliche Bestätigung durch den Auftraggeber mit Benennung der autorisierten Ansprechpartner vorgelegt werden.

3.2.2.2 Ablauf der Registrierung

1. Die Registrierungsunterlagen MÜSSEN persönlich durch einen Bevollmächtigten des Document Verifiers der CVCA-eID RA übergeben werden. Zu diesem Zeitpunkt wird keine Aussage über die Vollständigkeit und Korrektheit der Unterlagen gemacht.
2. Die CVCA-eID RA MUSS die Registrierungsunterlagen unter Einhaltung des 4-Augenprinzips sorgfältig prüfen.
   2.1. Sind die Unterlagen korrekt, wird Schritt 3 ausgeführt.
   2.2. Sind die Unterlagen fehlerhaft, MUSS die Registrierung unterbrochen werden. Der DV wird informiert und zur Nachbesserung aufgefordert. Bei schwerwiegenden Mängeln wird die Registrierung abgebrochen.
3. Die CVCA-eID RA MUSS die Registrierung im Registrierungsverzeichnis der CVCA-eID anlegen und die Daten so für den Wirkbetrieb nutzbar machen. Dabei MUSS im 4-Augenprinzip geprüft werden, dass weder die Authentizität noch die Integrität der Zertifikatsdaten verletzt wurde;
   3.1. Verläuft die Prüfung positiv, wird Schritt 4 ausgeführt.
   3.2. Wird eine Verletzung der Authentizität oder Integrität festgestellt, MUSS die Ursache der Abweichung ergründet werden. Danach kann bei erneuter Übergabe der Registrierungsunterlagen die Registrierung bei Schritt 2 fortgesetzt werden.
4. Das initiale DV-Zertifikat und das initiale MDS SubCA-Zertifikat werden ausgestellt. Nach Ausstellen des initialen DV-Zertifikats für eine BerCA MUSS die CVCA-eID die VfB über die Aufnahme des Wirkbetriebs des DV informieren.
5. Die initiale Registrierung ist abgeschlossen.

3.2.3 Registrierung von Terminals

Die Registrierungsinformationen über den Terminalbetreiber MÜSSEN im Registrierungsverzeichnis des DV vor dem Ausstellen des initialen Zertifikats erfasst werden.

3.2.3.1 Registrierungsunterlagen – alle Terminals

Die Registrierungsunterlagen **aller Terminals** MÜSSEN zumindest die folgenden Angaben beinhalten:

1. Name der Institution, die als Zertifikatsnehmer registriert werden möchte;
2. Kontaktdaten der Ansprechpartner;
3. Berechtigung des Terminalbetreibers zum Betrieb
   3.1. **hoheitliche Terminals:** Berechtigung des Terminalbetreibers zum Betrieb eines hoheitlichen Terminals (§36 (2) [PAuswV] bzw. §36 (1) 2 [PAuswV]);
   3.2. **nicht-hoheitliche Terminals:** Berechtigung des Diensteanbieters zum Erhalt von Berechtigungszertifikaten gemäß §21, §21a oder §21b [PAuswG] mit Informationen über den Typ des Diensteanbieters;
4. Informationen zur Art des Terminals:
   4.1. Integriertes oder verteiltes System, Einbindung eines Auftragnehmers, Einsatz von mobilen Lesegeräten oder EAC-Box etc.;
5. eindeutige Kennung des Terminals (z.B. Seriennummer oder Serverkennung)[12];
6. die für die Kommunikation gemäß [TR-03129] benötigten Daten (siehe Kapitel 1.4.5, „Kommunikation zwischen den Teilnehmern“):
   6.1. Adresse der Kommunikationsschnittstelle
   6.2. die für die Kommunikation genutzten Zertifikate (inklusive der zur Verifikation erforderlichen Zertifikatskette)
   6.3. Digitale Fingerprints der für die Kommunikation genutzten Zertifikate[13];
7. Erklärung zur Einhaltung der DV Policy;
8. initialer Zertifikatsrequest gemäß [TR-03110] oder alternativ in Abstimmung zwischen DV und Zertifikatsnehmer ein Request-Signer-Zertifikat für die Authentisierung von Zertifikatsanträgen;
9. digitaler Fingerprint des initialen Zertifikatsrequests oder alternativ in Abstimmung zwischen DV und Zertifikatsnehmer des Request-Signer-Zertifikats in gedruckter Form.
10. **nicht-hoheitliche Terminals, sofern eIDAS-Anwendungen bereitgestellt werden sollen:** initialer Zertifikatsrequest der Metadaten Signer sowie die zugehörigen Fingerprints.
11. **nicht-hoheitliche Terminals:** die notwendigen Informationen für die Certificate Description (siehe Kapitel 4.1.1.2.1)

3.2.3.2 Zusätzliche Informationen – Terminals mit Sicherheitslevel 2[14]

Zur Registrierung eines Terminals MUSS der Terminalbetreiber eine technische Beschreibung des Terminals beim DV einreichen, welche folgendes beinhaltet:

1. Hersteller und Modellbezeichnung;
2. Informationen zum Kryptografiemodul, inwiefern dies hinsichtlich Sicherheitseigenschaften geprüft wurde, z.B. Zertifizierung nach Common Criteria;
3. Nachweis der Zertifizierung der Betriebsumgebung (siehe auch Kapitel 5.1.1 und 6.2);

12 Für die Ausgabe von Terminalzertifikaten zum Zwecke der Qualitätssicherung anhand von Testausweisen gemäß §36 (1) 2 [PAuswV] entfällt die Benennung einer eindeutigen Terminalkennung.

13 In diesem Punkt DARF nach Rücksprache mit der CVCA eine Alternative gewählt werden, siehe auch Kapitel 3.2.3.4.

14 Definition der Sicherheitslevel siehe Kapitel 6 'Sicherheitsmaßnahmen für Schlüsselpaare'

3.2.3.3 Zusätzliche Informationen - EAC-Boxen gemäß [TR-03131]

EAC-Boxen gemäß [TR-03131] sind eine spezielle technische Ausprägung von Terminals, für sie gelten zusätzlich die folgenden Anforderungen.

Bei der Produktion einer EAC-Box wird diese mit einem privaten Schlüssel ($SKey_{EAC\text{-}Box}$) zur Signatur des initialen Zertifikatsrequests versehen. Der zugehörige öffentliche Schlüssel ($PKey_{EAC\text{-}Box}$) wird im Registrierungsverzeichnis des zuständigen DVs unter der Registrierung des entsprechenden Terminals hinterlegt. Zusätzlich werden Kommunikationszertifikate für eine sichere Kommunikation hinterlegt.

Die Identifizierung und Authentifizierung eines initialen Zertifikatsrequests durch den DV erfolgt dann wie folgt:

1. Die TLS-Verbindung zum hoheitlichen DV MUSS mittels der hinterlegten Kommunikationszertifikate authentisiert werden.
2. Der Zertifikatsrequest MUSS mit $SKey_{EAC\text{-}Box}$ signiert sein. Die Prüfung erfolgt mit $PKey_{EAC\text{-}Box}$ aus dem Verzeichnisdienst des DV, der für das entsprechende Terminal registriert sein MUSS.
3. Das CHR-Feld des Zertifikatsrequests MUSS den beim DV registrierten Holder Mnemonic beinhalten.

3.2.3.4 Pflichten der Document Verifier

Im Rahmen der Registrierung eines Terminalbetreibers MUSS der DV die folgenden Pflichten wahrnehmen:

1. Die Vollständigkeit und Konsistenz der Registrierungsinformationen sorgfältig prüfen; hier insbesondere die Berechtigung des Terminalbetreibers zum Betrieb.
2. Prüfen, ob Integrität und Authentizität der bei der Registrierung übergebenen Zertifikate bzw. Zertifikatsrequests intakt sind. Im Regelfall SOLLTE dies über die Prüfung der Fingerprints der Kommunikationszertifikate und des initialen Zertifikatsrequests bzw. des Request-Signer-Zertifikats gegen die jeweiligen Zertifikate bzw. Zertifikatsrequests erfolgen[15]. Führt diese Prüfung zu einem negativen Ergebnis, MUSS die Ursache dafür geklärt und behoben werden und die Registrierungsinformationen MÜSSEN erneut ausgetauscht und geprüft werden.
3. **Nur Terminals mit Sicherheitslevel 2:** Prüfen, ob die Unterlagen zur technischen Beschreibung des Terminals (siehe Kapitel 3.2.3.2) vollständig vorliegen.
4. Die Registrierungsinformationen korrekt in das Registrierungsverzeichnis eintragen.
5. **Nur Terminals mit Sicherheitslevel 2:** die Unterlagen zur technischen Beschreibung des Terminals hinterlegen.

Zusätzliche Prüfungen nicht-hoheitliche DV

Der DV MUSS zusätzlich folgendes prüfen:

1. Berechtigung des Diensteanbieters durch die VfB liegt vor;
2. Die Informationen zur Identifizierung des Diensteanbieters in den Registrierungsinformationen des DV und die der VfB stimmen überein;
3. Korrektheit der Angaben für die Certificate Description (siehe Kapitel 4.1.1.2.1);
4. Konfiguration der Berechtigungen für die Terminal-Zertifikate nach den Vorgaben der VfB für den Diensteanbieter.

15 Wird ein anderer Prozess zur Prüfung der Integrität und Authentizität gewählt, z.B. wegen Nutzung intern erstellter TLS-Zertifikate, MUSS dieser in der CP des DV beschrieben sein.

4 Zertifikatslebenszyklus

4.1 Zertifikatsprofile

4.1.1 Zertifikatsprofile für die CV-Zertifikate

Die in der CVCA-eID PKI verwendeten Zertifikate sind selbst-beschreibende Card Verifiable Zertifikate (CV-Zertifikate) gemäß [TR-03110]. Das Profil eines Zertifikatsrequests oder Zertifikats MUSS konform zu [TR-03110] sein.

Die Ausstellung und Validierung der Zertifikate MUSS auf dem Schalenmodell basierend erfolgen.

Zur Erzeugung von Schlüsselpaaren MÜSSEN die, in der jeweils aktuellen Version der [TR-03116-2][16] vorgegebenen, kryptografischen Verfahren und Schlüssellängen verwendet werden.

Darüber hinaus MÜSSEN zusätzliche Anforderungen für die Belegung folgender Zertifikatsfelder eingehalten werden:

- Die „Certificate Holder Reference" bezeichnet den Antragssteller (siehe Kapitel 3.1)
- Das „Certificate Effective Date" und das „Certificate Expiration Date" bilden zusammen den Gültigkeitszeitraum des Zertifikats (siehe Kapitel 4.7)
- Das „Certificate Holder Authorization Template" beinhaltet die relativen Zugriffsrechte des Zertifikats (siehe Kapitel 4.1.1.1)
- Die „Certificate Extensions" enthalten die Zertifikatserweiterungen (siehe Kapitel 4.1.1.2)

4.1.1.1 Zugriffsrechte

In den Zertifikaten werden die Zugriffsrechte gemäß [TR-03110] durch den Zertifikatsaussteller im „Certificate Holder Authorization Template" (CHAT) verankert. Dabei werden die maximalen Zugriffsrechte durch das entsprechende CVCA Zertifikat bestimmt, diese können durch die im DV Zertifikat gesetzten Rechte lediglich weiter eingeschränkt werden. Mit dem Terminal Zertifikat ist dann eine weitere Einschränkung der Zugriffsrechte aus dem zugehörigen DV Zertifikat möglich.

Welche Zugriffsrechte in einem Zertifikat gewährt werden dürfen, ist durch das [PAuswG] bzw. das [AufenthG] geregelt.

Zugriffsrechte für Diensteanbieter

Die Zugriffsrechte für die einzelnen Datengruppen und Funktionen der Diensteanbieter werden von der VfB als Registrierungsinstanz festgelegt und von dem zuständigen DV im Terminal-Zertifikat entsprechend verankert.

Dabei wird zunächst entschieden, ob es sich um

- einen Diensteanbieter für den elektronischen Identitätsnachweis, d.h. einen Diensteanbieter gemäß nach §21 [PAuswG] bzw. einen Identifizierungsdiensteanbieter nach §21b [PAuswG], oder um
- einen Diensteanbieter für das Vor-Ort-Auslesen nach §21a [PAuswG]

handelt. Anhand dieser Kategorien können die Zugriffsrechte dann gemäß dem Bescheid der VfB individuell für den Diensteanbieter festgelegt werden.

Die BerCA MUSS durch geeignete technische und / oder organisatorische Maßnahmen sicherstellen, dass Diensteanbieter im Berechtigungszertifikat nur Zugriffsrechte gemäß dem Bescheid der VfB erhalten. Dabei gilt:

- Diensteanbieter für den **elektronischen Identitätsnachweis** KANN das Recht **„Installation qualifiziertes Signaturzertifikat"** erhalten und DARF NICHT das Recht „CAN allowed" erhalten.
- **Vor-Ort-Auslesen** MUSS das Recht **„CAN allowed"** haben und DARF NICHT das Recht „Installation qualifiziertes Signaturzertifikat" erhalten;

16 siehe https://www.bsi.bund.de/ElektronischeAusweiseTR

Insbesondere **DÜRFEN die Rechte „Installation qualifiziertes Signaturzertifikat“ und „CAN allowed“ NICHT im selben Terminal-Zertifikat gesetzt** sein.

Die Angabe „Nachladen der qualifizierten Signatur auf dem Personalausweis“ als Verwendungszweck im Bescheid der VfB bezieht sich auf die Rechte zur Installation eines qualifizierten Signaturzertifikats.

Tabelle 4 zeigt eine Übersicht der Verteilung der Zugriffsrechte in den Zertifikaten der CVCA-eID und der Document Verifier.

Datengruppe	CVCA-eID	DV Hoheitlich	DV Nicht-Hoheitlich (BerCA)
Schreibzugriff			
DG 17 (Anschrift)	Ja	Ja	Nein
DG 18 (Wohnort-ID)	Ja	Ja	Nein
DG 19 (Nebenbestimmungen I - eAT)	Ja	Ja	Nein
DG 20 (Nebenbestimmungen II - eAT)	Ja	Ja	Nein
DG 21 (unbenutzt)	-	-	-
Lesezugriff			
DG 21 (unbenutzt)	-	-	-
DG 20 (Nebenbestimmungen II - eAT)	Ja	Ja	Nein
DG 19 (Nebenbestimmungen I - eAT)	Ja	Ja	Ja
DG 18 (Wohnort-ID)	Ja	Ja	Ja
DG 17 (Anschrift)	Ja	Ja	Ja
DG 16 (unbenutzt)	-	-	-
DG 15 (unbenutzt)	-	-	-
DG 14 (unbenutzt)	-	-	-
DG 13 (Geburtsname)	Ja	Ja	Ja
DG 12 (unbenutzt)	-	-	-
DG 11 (unbenutzt)	-	-	-
DG 10 (Staatsangehörigkeit)	Ja	Ja	Ja
DG 9 (Geburtsort)	Ja	Ja	Ja
DG 8 (Geburtsdatum)	Ja	Ja	Ja
DG 7 (Doktorgrad)	Ja	Ja	Ja
DG 6 (Ordens-/Künstlername)	Ja	Ja	Ja
DG 5 (Familienname)	Ja	Ja	Ja
DG 4 (Vorname(n))	Ja	Ja	Ja
DG 3 (Ablaufdatum)	Ja	Ja	Ja
DG 2 (Ausgebender Staat)	Ja	Ja	Ja
DG 1 (Dokumententyp)	Ja	Ja	Ja
Spezielle Funktionen			
Installation qualifiziertes Signaturzertifikat	Ja	Nein	Ja
Installation Signaturzertifikat	Ja	Nein	Nein
PIN-Management	Ja	Ja	Nein
CAN allowed	Ja	Ja	Ja
Privilegiertes Terminal	Ja	Ja	Nein
Pseudonym	Ja	Ja	Ja
Wohnortsverifikation	Ja	Ja	Ja
Altersverifikation	Ja	Ja	Ja

Tabelle 4: Zugriffsrechte für CVCA- und DV-Zertifikate

Tabelle 5 gibt eine Übersicht über die Zugriffsrechte für hoheitliche Online-Dienste in der CVCA-eID Infrastruktur.

Datengruppe	Ummelde-/ Schreibdienst (hoheitlich)	PIN-Rücksetzdienst (hoheitlich)
Schreibzugriff		
DG 17 (Anschrift)	Ja	Nein
DG 18 (Wohnort-ID)	Ja	Nein
DG 19 (Nebenbestimmungen I - eAT)	Nein	Nein
DG 20 (Nebenbestimmungen II - eAT)	Nein	Nein
DG 21 (unbenutzt)	-	-
Lesezugriff		
DG 21 (unbenutzt)	-	-
DG 20 (Nebenbestimmungen II - eAT)	Nein	Nein
DG 19 (Nebenbestimmungen I - eAT)	Nein	Nein
DG 18 (Wohnort-ID)	Ja	Nein
DG 17 (Anschrift)	Ja	Ja
DG 14 - 16 (unbenutzt)	-	-
DG 13 (Geburtsname)	Ja	Nein
DG 11 - 12 (unbenutzt)	-	-
DG 10 (Staatsangehörigkeit)	Nein	Nein
DG 9 (Geburtsort)	Ja	Nein
DG 8 (Geburtsdatum)	Ja	Ja
DG 7 (Doktorgrad)	Nein	Nein
DG 6 (Ordens-/Künstlername)	Nein	Nein
DG 5 (Familienname)	Ja	Ja
DG 4 (Vorname(n))	Ja	Ja
DG 3 (Ablaufdatum)	Nein	Nein
DG 2 (Ausgebender Staat)	Nein	Nein
DG 1 (Dokumententyp)	Ja	Ja
Spezielle Funktionen		
Installation qualifiziertes Signaturzertifikat	Nein	Nein
Installation Signaturzertifikat	Nein	Nein
PIN-Management	Nein	Ja
CAN allowed	Nein	Ja
Privilegiertes Terminal	Ja	Ja
Pseudonym	Nein	Ja
Wohnortsverifikation	Nein	Nein
Altersverifikation	Nein	Ja
Certificate Extensions[17]		

Tabelle 5: Zugriffsrechte für hoheitliche Online-Dienste

4.1.1.2 Zertifikatserweiterungen CV-Zertifikate

Jedes CV-Zertifikat, welches von einer BerCA oder einem hoheitlichen DV für hoheitliche Online-Dienste ausgestellt wird, MUSS die folgenden „Certificate Extensions" gemäß [TR-03110] enthalten:

- Certificate Description;
- Terminal Sector.

Zertifikatserweiterungen, die über die oben aufgeführten hinausgehen, MÜSSEN mit der CVCA-eID abgestimmt werden.

17 Siehe Kapitel 4.1.1.2 für die benötigten Certificate Extensions für die hoheitlichen Online-Dienste

4.1.1.2.1 Certificate Description Extension

Die Certificate Description Extension enthält Informationen zum Diensteanbieter (Hashwert der Datenstruktur CertificateExtension nach [TR-03110]). Der Inhalt MUSS dem, in der durch die VfB erteilten Berechtigung enthaltenen, Inhalt entsprechen.

Für die Felder der `CertificateDescription` gelten die folgenden Anforderungen:

- `issuerName` MUSS den Namen der ausstellenden BerCA enthalten.
- `issuerURL` kann eine Web- oder Email-Adresse der BerCA in Form einer URL enthalten.
- `subjectName` MUSS den Namen des Diensteanbieters gemäß Bescheid der VfB enthalten.
- `termsOfUsage`
  - MUSS im Plain Text Format gemäß [TR-03110] codiert sein. Die Alternativen HTML Format oder PDF Format DÜRFEN NICHT gewählt werden.
  - MUSS die folgenden Angaben zum Diensteanbieter (sofern vorhanden, jeweils getrennt durch eine Leerzeile) gemäß Bescheid der VfB enthalten:
    - „Name, Anschrift und E-Mail-Adresse des Diensteanbieters:
      <Wert>“„
    - Im Falle eines Identifizierungs- oder Vor-Ort-Diensteanbieters:
      „Informationen über den Typ des Diensteanbieters:
      <Wert>“,
    - Im Falle von Berechtigungen, die vor dem 15.07.2017 ausgesprochen wurden:
      „Geschäftszweck: Zweck der Übermittlung
      <Wert>“,
    - „Hinweis auf die für den Diensteanbieter zuständigen Stellen, die die Einhaltung der Vorschriften zum Datenschutz kontrollieren:
      <Wert>“.

Für Zertifikate, die für Online-Anwendungen ausgestellt werden, MUSS die `CertificateDescription` die folgenden Felder enthalten:

- `subjectURL` MUSS die Web-Adresse des Diensteanbieters für den gemäß Bescheid der VfB berechtigten Dienst als URL enthalten. Die enthaltene URL MUSS eine https-URL sein und MUSS nach den Regeln in [RFC6454] zu der Webseite gehören, auf der die Online-Authentisierung durchgeführt wird (siehe auch [TR-03124-1]).
- `commCertificates` MUSS die Hash-Werte aller der für die Kommunikation zwischen Diensteanbieter/eID-Server einerseits und eID-Client andererseits verwendeten TLS-Zertifikate enthalten (siehe auch [TR-03124-1]). Die BerCA MUSS sorgfältig die Authentizität der TLS-Zertifikate prüfen und sicherstellen, dass die korrekten Hash-Werte dieser Zertifikate in die Extension aufgenommen werden. Dies schließt die Prüfung ein, dass alle in den Zertifikaten enthaltenen Domain-Namen[18] unter der Kontrolle des Diensteanbieters bzw. eines beauftragten Datenverarbeiters stehen. Des weiteren MUSS die BerCA prüfen, dass die in den TLS-Zertifikaten enthaltenen kryptographischen Parameter (Schlüssellängen, Signaturalgorithmus) den Anforderungen der [TR-03116-4] entsprechen.

4.1.1.2.2 Terminal Sector Extension

Diese Extension enthält den oder die Sector Public Key IDs[19] für den oder die Sector Public Key(s) des Diensteanbieters für die Erzeugung von Sperrmerkmal und Pseudonym.

18 Gemäß [RFC6454] werden für den Vergleich das Protokoll, der Port und der Host-Anteil der URL genutzt. Weitere Bestandteile der URL werden ignoriert. Für Details siehe [RFC6454].

19 Eine Sector Public Key ID ist der Hashwert eines Sector Public Keys, vgl. [TR-03110], Teil 3.

Die entsprechenden Schlüsselpaare MÜSSEN durch die BerCA sowie durch einen hoheitlichen DV für die Online-Dienste aus Tabelle 5 erzeugt werden. Diese hoheitlichen DVs und BerCAs MÜSSEN zwei Sector Public Key IDs in den Zertifikaten unterstützen. Sofern die Extension zwei Sector Public Key IDs enthält (z.B. für eine Migration, siehe Kapitel 4.1.1.2.3), so MUSS die ID des neuesten Sector Public Keys an erster Stelle stehen.

Zu einem Sector Public Key, mit dem das Sperrmerkmal berechnet wird (d.h. den neuesten Sector Public Key), benötigen die BerCA sowie die hoheitlichen DVs, die Zertifikate für hoheitliche Online-Terminals ausstellen, auch den privaten Schlüssel. Der private Schlüssel MUSS durch die BerCA sowie die hoheitlichen DVs für den Ummelde-/Schreibdienst und den PIN-Rücksetzdienst für die Berechnung von dienstespezifischen Sperrlisten gespeichert werden (siehe [TR-03127]). Der private Schlüssel MUSS unter Einhaltung der Anforderungen aus Kapitel 6 „Sicherheitsmaßnahmen für Schlüsselpaare“ sicher gespeichert werden und DARF dem Diensteanbieter NICHT bekannt sein (siehe 6.3 „Berechnung von Sperrlisten für eID-Dokumente“).

4.1.1.2.3 Migration des Terminal Sectors

In verschiedenen Situationen ist die Migration bzw. Wechsel des Terminal Sectors notwendig, z.B.:

1. Wechsel des globalen Schlüsselpaares für den Sperrsektor (ggf. incl. Wechsel der Domainparameter);
2. Zusammenführung von Pseudonymen zweier Dienste, wenn diese Dienste zu einem Dienst zusammengelegt werden;
3. Wechsel eines Diensteanbieters zu einer anderen BerCA;
4. Wechsel des Betreibers eines hoheitlichen DVs.

Für den Wechsel eines Terminal Sectors sehen die Spezifikationen des Ausweises und der Infrastruktur die Möglichkeit vor, mehrere (zwei) Sector Public Key IDs in das Berechtigungszertifikat aufzunehmen.

Führt der Wechsel des Terminal Sectors bei einem Diensteanbieter bei der Verwendung der Pseudonym-Funktion zur Erzeugung neuer Pseudonyme (etwa in den Bsp. 2 und 3 oben), wird der Einsatz einer der folgenden Varianten zur Migration empfohlen.

Variante 1: Neue Pseudonyme

Neuregistrierung der Anwender bzw. der Pseudonyme beim Diensteanbieter, etwa durch erneutes Auslesen der personenbezogenen Daten (sofern per Berechtigung verfügbar). Dies entspricht prozedural der Situation eines neuen Ausweises beim Bürger.

Variante 2: Migration der Sector Public Keys

Berechtigungszertifikate können zwei Sector Public Key IDs enthalten, um einen Wechsel des Terminal Sectors zu ermöglichen. Dazu ist notwendig:

- Der eID-Server muss die Abfrage des Sperrmerkmals und des Pseudonyms mit mehreren Sector Public Keys unterstützen (vgl. [TR-03130] Abschnitt 4.3.2 und [TR-03110] Abschnitt B.4).
- Bei der Migration zu einer anderen BerCA: Der Sector Public Key muss zur neuen BerCA übertragen werden. Dies kann manuell geschehen, ein automatisierter Prozess ist nicht notwendig. Da der Key grundsätzlich dem Diensteanbieter bzw. dem eID-Server bekannt ist, kann dies auch ohne aktive Mitwirkung der alten BerCA geschehen.

In der [TR-03130] Teil 1 ist festgelegt, dass der eID-Server zwei Pseudonyme von der Karte abruft, wenn im Berechtigungszertifikat zwei Sector Public Key IDs enthalten sind, d.h. die Steuerung der Erzeugung zweier Pseudonyme erfolgt über die von der BerCA ausgestellten Berechtigungszertifikate.

Die BerCA MUSS den Diensteanbieter darauf hinweisen, dass es sinnvoll ist, wenn der Diensteanbieter seine Pseudonym-Datenbank mittels dieses Verfahrens von den alten Pseudonymen auf die neuen migriert, damit nicht dauerhaft Pseudonyme für zwei Terminal Sectors erzeugt werden müssen.

Die Dauer, für die zwei Pseudonyme erzeugt werden, MUSS zwischen Diensteanbieter und BerCA verabredet werden. Grundsätzlich ist auch eine dauerhafte Erzeugung des alten Pseudonyms denkbar (dann muss

der Diensteanbieter seine Datenbank nicht migrieren). Es muss beachtet werden, dass solange der alte Sector Public Key im Zertifikat enthalten ist, keine anderen Migrationen (siehe oben) möglich sind.

Variante 3: Übertragung des Sector Private Keys (nur für BerCA-Wechsel)

Alternativ kann auch der Sector Private Key von der alten BerCA zur neuen übertragen werden. Dafür muss eine geeignete Methode gemäß Kapitel 6 gewählt werden. Zusätzlich MUSS der private Schlüssel nach erfolgreichem Transfer bei der alten BerCA gelöscht werden (siehe auch Kapitel 6).

4.1.2 Zertifikatsprofile für die MDS-Zertifikate

Die MDS-Zertifikate sind X.509 Zertifikate gemäß [RFC5280]. Des Weiteren MÜSSEN die Vorgaben aus [eIDAS-Crypto] für X.509 Zertifikate und die Vorgaben aus dieser Certificate Policy eingehalten werden.

Jedes MDS Zertifikat MUSS die „`CRLDistributionPoints`“ Extension gemäß [RFC5280] beinhalten. Mindestens ein in der Extension genannter CRL Distribution Point MUSS über http frei erreichbar sein.

Die Algorithmen und Schlüssellängen für MDS-Zertifikate MÜSSEN gemäß den Vorgaben aus [TR-03116-2] gewählt werden.

4.1.3 Signieren von Metadaten

Beim Signieren von Metadaten MUSS der Diensteanbieter sicherstellen, dass die Metadaten die Anforderungen von [eIDAS-SAML] erfüllen und dass die enthaltenen Informationen im Hinblick auf den Dienst korrekt sind.

4.2 Initiale Zertifikatsanträge

4.2.1 Initiale Zertifikatsanträge für CV-Zertifikate

Ein **initialer Zertifikatsrequest** eines DV oder Terminals ist definiert als:

- der erste Zertifikatsrequest dieses Zertifikatsnehmers unter der Zertifizierungsinstanz oder
- der erste Zertifikatsrequest nach Aufhebung einer Sperrung dieses Zertifikatsnehmers oder
- ein neuer Zertifikatsrequest, für den kein gültiges Zertifikat[20] vorliegt, mit dem der Request authentisiert werden kann.

Es wird zwischen folgenden Arten von initialen Zertifikatsrequests unterschieden (vgl. [TR-03110] Part 3, Kapitel C.2):

- **Initialer Zertifikatsrequest ohne äußere Signatur**:
  - Zum initialen Zertifikatsrequest ohne äußere Signatur MUSS der digitale Fingerprint des Zertifikatsrequests auf einem zweiten Kanal oder Medium übergeben werden.
- **Initialer Zertifikatsrequest mit äußerer Signatur**:
  - Alternativ KANN in Abstimmung zwischen Registrierungsinstanz und Zertifikatsnehmer ein vorab registriertes Request-Signer-Zertifikat für die äußere Signatur zur Authentisierung des initialen Zertifikatsrequests verwendet werden. In diesem Fall MUSS der initiale Zertifikatsrequest die äußere Signatur mit dem gültigen privaten Schlüssel des Request-Signer-Zertifikats des Antragsstellers enthalten.

Für jeden Zertifikatsrequest MUSS ein neues Schlüsselpaar generiert werden. Die Beantragung und Ausstellung eines initialen Zertifikats MUSS gemäß Kapitel 4.4 „Beantragung und Ausstellung von Zertifikaten“ erfolgen.

Für eine wiederholte[21] Beantragung eines **initialen** Zertifikats MUSS eine der folgenden Gegebenheiten vorliegen und die zugehörigen Bedingungen MÜSSEN eingehalten werden:

20 d.h. vorhergehendes CV-Zertifikat oder nach Abstimmung mit der CA ein Request-Signer-Zertifikat

21 d.h. der Antragssteller hat schon einmal ein korrektes initiales Zertifikat erhalten.

- Im Falle eines vorhergegangenen Sicherheitsvorfalls, wie z.B. einer Kompromittierung des privaten Schlüssels, MUSS zunächst die Ursache des Sicherheitsvorfalls gefunden und das korrespondierende Sicherheitsproblem gelöst werden. Die Registrierungsinstanz (CVCA-RA bzw. DV und VfB) MUSS vor Bearbeitung eines neuen Zertifikatsrequests darüber entscheiden, ob die Sicherheitsmaßnahmen ausreichend nachgebessert wurden.
- Im Falle eines wiederholten initialen Zertifikatsrequests, für den kein gültiges Zertifikat[22] vorliegt, mit dem der Antrag authentisiert werden kann, (z.B. weil der Schlüsselspeicher defekt ist) MUSS der Antragsteller die Gründe für den verspäteten Antrag angeben. Hier kann die Registrierungsinstanz OPTIONAL auch hier eine Nachbesserung des Verfahrens beim Antragsteller verlangen.
- In jedem Fall MÜSSEN für einen wiederholten initialen Zertifikatsrequest dieselben Anforderungen beachtet werden wie für den ersten initialen Zertifikatsrequest (siehe Kapitel 4.4 „Beantragung und Ausstellung von Zertifikaten“).

4.2.2 Initiale Zertifikatsanträge für MDS-Zertifikate

Die Zertifikatsanträge MÜSSEN im PKCS#10 Format gemäß [RFC2986] erstellt und der jeweiligen CA übermittelt werden. Zudem MUSS der digitale Fingerprint des Zertifikatsantrags auf einem zweiten Kanal übermittelt werden (z.B. kann der Zertifikatsantrag per E-Mail versendet werden und der Fingerprint per Telefon).

Des Weiteren MÜSSEN die Zertifikatsanträge Werte für das Feld „Subject“ unter Berücksichtigung der Vorgaben für die Namensgebung (siehe Kapitel 3.1.2) sowie die Extension „CRL Distribution Point“ beinhalten.

Der Wert des Feldes „CRL Distribution Point“ MUSS auf die Adresse der Zertifikats-Sperrliste verweisen, auf welcher ein Sperreintrag für das vorliegende Zertifikat im Sperrfall vermerkt wird.

4.3 Wiederholungsanträge

4.3.1 Wiederholungsanträge für CV-Zertifikate

Ein Wiederholungsantrag ist ein Zertifikatsrequest desselben Antragsstellers, der kein initialer Zertifikatsrequest ist (siehe oben stehende Definition). Ein Folgezertifikat ist ein Zertifikat, welches auf Basis eines Wiederholungsantrages ausgestellt wird.

Für einen Wiederholungsantrag MUSS eine der folgenden Bedingungen gelten

- der Gültigkeitszeitraum des aktuellen DV- oder Terminal-Zertifikats ist fast beendet, hierfür sind die Reaktionszeiten in Kapitel 4.4 „Beantragung und Ausstellung von Zertifikaten“ zu beachten oder
- die Zugriffsrechte in den Zertifikaten des Antragsstellers sollen geändert werden.

Ein **Wiederholungsantrag MUSS abgelehnt** werden, wenn

- die Registrierung des Antragstellers zwischen der Ausstellung des letzten Zertifikats und der Einreichung des aktuellen Zertifikatsrequests gesperrt war;
- der Antragsteller nicht in der Lage ist, den Zertifikatsrequest mit einem bei der CA registrierten, noch gültigen privaten Schlüssel zu signieren.

(in diesen Fällen siehe Kapitel 4.2.1 „Initiale Zertifikatsanträge für CV-Zertifikate“).

Für den Wiederholungsantrag MÜSSEN die folgenden Bedingungen eingehalten werden:

- der Antragssteller hat ein neues Schlüsselpaar für den Zertifikatsrequest generiert;
- der Zertifikatsrequest enthält eine andere (nachfolgende) Seriennummer im CHR (siehe Kapitel 3.1) als die vorherigen Zertifikate des Antragsstellers;
- Die Integrität und Authentizität eines Wiederholungsantrags MUSS gemäß [TR-03110] durch eine Signatur mit dem jeweiligen privaten Schlüssel des bei der CA registrierten, noch gültigen Zertifikats des Antragsstellers prüfbar sein (siehe [TR-03110] Part 3, C.2 „successive certificate“). Hierbei sind folgende Verfahren erlaubt:

22 d.h. vorhergehendes CV-Zertifikat oder nach Abstimmung mit der CA ein Request-Signer-Zertifikat

- Wiederholungsantrag mit gültigen CV-Zertifikat
  - Der Zertifikatsrequest MUSS mit einem, noch gültigen[23], privaten Schlüssel eines vorhergehenden CV-Zertifikats desselben Antragsstellers signiert werden.
- Wiederholungsantrag mit registriertem gültigen Request-Signer-Zertifikat:
  - Alternativ zu dem oben genannten Verfahren KANN[24] in Abstimmung zwischen Registrierungsinstanz und Zertifikatsnehmer ein vorab registriertes Request-Signer-Zertifikat für die äußere Signatur zur Authentisierung des Wiederholungsantrags verwendet werden. In diesem Verfahren MÜSSEN die Wiederholungsanträge die äußere Signatur mit dem gültigen privaten Schlüssel des Request-Signer-Zertifikats desselben Antragsstellers enthalten.
- Diensteanbieter stellen ihre Wiederholungsanträge direkt an die BerCA, welche die entsprechenden Prüfungen durchführt.
- Das Zertifikat wird unter Einhaltung der Vorgaben für Wiederholungsanträge aus Kapitel 4.4 „Beantragung und Ausstellung von Zertifikaten“ erstellt.

4.3.2 Wiederholungsanträge für MDS-Zertifikate

Wiederholungsanträge für MDS SubCA-Zertifikate entsprechen den initialen Zertifikatsanträgen für MDS-Zertifikate (siehe Kapitel 4.2.2).

Wiederholungsanträge für MDS-Zertifikate von Terminals KÖNNEN auf mittels der Kommunikationsschnittstelle gemäß [TR-03129] gestellt werden (siehe Kapitel 1.4.5 „Kommunikation zwischen den Teilnehmern“).

4.4 Beantragung und Ausstellung von Zertifikaten

Jeder, der Zertifikatsrequests stellen möchte, MUSS den Registrierungsprozess (Kapitel 3.2 „Registrierung“) erfolgreich durchlaufen haben.

4.4.1 Beantragung von CV-Zertifikaten

Genereller Beantragungsprozess

Im Folgenden wird der Beantragungsprozess eines DV- oder Terminal-Zertifikats beschrieben und die dabei zu beachtenden Vorgaben für **Zertifikatsnehmer** und **Zertifizierungsinstanz** werden festgelegt:

1. Generieren des Schlüsselpaares:
   1.1. Der **Zertifikatsnehmer** MUSS ein Schlüsselpaar gemäß [TR-03110] generieren und MUSS dabei die Anforderungen aus den Kapiteln 5 „Sicherheitsmaßnahmen“ und 6 „Sicherheitsmaßnahmen für Schlüsselpaare“ berücksichtigen.
2. Generieren des Zertifikatsrequests:
   2.1. Der **Zertifikatsnehmer** generiert einen Zertifikatsrequest, welcher den neuen öffentlichen Schlüssel und eine innere Signatur (siehe [TR-03110]) auf Basis des zugehörigen privaten Schlüssels beinhalten MUSS. Die Erstellung des Zertifikatsrequests MUSS unter Berücksichtigung der Vorgaben aus Kapitel 3.1 „Namensgebung“ sowie [TR-03110] erfolgen.
3. **Nur initialer Zertifikatsrequest mit äußerer Signatur oder Wiederholungsantrag:** Generieren der äußeren Signatur
   3.1. Der Zertifikatsrequest MUSS eine äußere Signatur gemäß [TR-03110] erhalten[25].

23 siehe Kapitel 4.4.1.2 „Beantragungszeiten“

24 Es wird empfohlen, dass der Zertifikatsnehmer und die Registrierungsinstanz sich grundsätzlich auf eines der beiden Verfahren einigen.

25 Sollte keine der beiden Varianten für Wiederholungsanträge möglich sein (z.B. weil der Zertifikatsrequest nicht rechtzeitig generiert wurde), muss die CVCA-eID informiert und ein neuer initialer Zertifikatsrequest gestellt werden. Ist ein Wiederholungsantrag mit registriertem gültigen Request-Signer-Zertifikat unmöglich

3.1.1. **Initialer Zertifikatsantrag mit äußerer Signatur**: Der Request MUSS mithilfe des privaten Schlüssels zum Request-Signer-Zertifikat erstellt werden.

3.1.2. **Wiederholungsantrag mit gültigem CV-Zertifikat**: Der Request MUSS mithilfe des privaten Schlüssels des noch gültigen Vorgänger-Zertifikats erstellt werden.

3.1.3. **Wiederholungsantrag mit registriertem gültigen Request-Signer-Zertifikat**: Der Request MUSS mithilfe des privaten Schlüssels zum Request-Signer-Zertifikat erstellt werden.

4. Zertifikatsrequest übermitteln:
   - 4.1. **Initialer Zertifikatsrequest ohne äußere Signatur:** Der initiale Zertifikatsrequest MUSS durch den **Zertifikatsnehmer** in einer Form übermittelt werden, die die Prüfung der Authentizität und Integrität des Zertifikatsrequests ermöglicht.
   - 4.2. **Initialer Zertifikatsrequest mit äußerer Signatur oder Wiederholungsantrag:** Bei der Übermittlung des Zertifikatsrequests durch den **Zertifikatsnehmer** an die zuständige Zertifizierungsinstanz MÜSSEN die Vorgaben aus Kapitel 1.4.5 „Kommunikation zwischen den Teilnehmern“ eingehalten werden.
5. Zertifikatsrequest prüfen:
   - 5.1. **Initialer Zertifikatsrequest ohne äußere Signatur:** Die **Zertifizierungsinstanz** MUSS sorgfältig prüfen, ob die Authentizität und Integrität des Zertifikatsrequests unverfälscht sind und der Zertifikatsrequest konform zu den Vorgaben aus 3.1 „Namensgebung“ sowie [TR-03110] ist.
   - 5.2. **Initialer Zertifikatsrequest mit äußerer Signatur oder Wiederholungsantrag:** Die **Zertifizierungsinstanz** MUSS sorgfältig prüfen, ob die äußere Signatur des Zertifikatsrequests korrekt und der Zertifikatsrequest konform zu den Vorgaben aus 3.1 „Namensgebung“ sowie [TR-03110] ist.
6. Registrierungsstatus prüfen:
   - 6.1. Die **Zertifizierungsinstanz** MUSS prüfen, ob der Zertifikatsnehmer aktuell berechtigt ist, Zertifikate zu erhalten und ob die Registrierungsinformationen über den Zertifikatsnehmer aktuell sind. Wenn vorhanden, MUSS die Zertifizierungsinstanz die Korrektheit der Angaben für die Certificate Description (siehe Kapitel 4.1.1.2.1) zum Zertifikatsrequest prüfen.
7. Zertifikat ausstellen:
   - 7.1. Die **Zertifizierungsinstanz** DARF KEIN Zertifikat auf Basis des Zertifikatsrequests ausstellen, wenn einer der beiden oder beide vorherigen Schritte zu einem negativen Ergebnis geführt hat. In diesem Fall MUSS die Zertifizierungsinstanz den Zertifikatsrequest ablehnen.
8. Antwort übermitteln:
   - 8.1. Die **Zertifizierungsinstanz** MUSS den Zertifikatsrequest beantworten und MUSS dabei die Vorgaben aus Kapitel 1.4.5 „Kommunikation zwischen den Teilnehmern“ einhalten. Die Antwort enthält entweder das Zertifikat oder die Ablehnung des Zertifikatsrequests.
9. Zertifikat annehmen:
   - 9.1. Der **Zertifikatsnehmer** MUSS das erhaltene Zertifikat in sein Zertifikatsverwaltungssystem unter Berücksichtigung der Vorgaben von Kapitel 2.1 „Zertifikatsverzeichnisse“ integrieren.
10. Löschen des alten Schlüssels:
    - 10.1. Wenn das neue Zertifikat erfolgreich in das Zertifikatsverwaltungssystem des Zertifikatsnehmers integriert werden konnte und der zugehörige private Schlüssel aktiviert wird (siehe Kapitel 6, „Sicherheitsmaßnahmen für Schlüsselpaare“), MUSS dieser den privaten Schlüssel des Vorgängerzertifikats unter Berücksichtigung der Vorgaben aus Kapitel 6, „Sicherheitsmaßnahmen für Schlüsselpaare“löschen.
    - 10.2. Andernfalls muss ein neuer Zertifikatsrequest generiert und sämtliche Schritte zur Beantragung erneut durchlaufen werden.

Die beschriebenen manuellen Schritte SOLLEN auf Basis des 4-Augenprinzips durchgeführt werden.

geworden, muss auch ein neues Request-Signer-Zertifikat analog zur Registrierung gemäß Kapitel 3.2 „Registrierung“.

4.4.1.1 Zertifikate der CVCA

Bei der Aufnahme des Wirkbetriebs generiert die CVCA-eID das initiale **Root-Schlüsselpaar** und ein zugehöriges selbst-signiertes Zertifikat.

- Zertifikatsanträge für CVCA-Zertifikate werden von der CVCA-eID selbst getätigt.
- Vor Ablauf des aktiven Root-Schlüsselpaars MUSS ein neues Root-Schlüsselpaar erzeugt werden.
- Zu jedem Root-Schlüsselpaar nach dem initialen Schlüsselpaar MÜSSEN ein CVCA- und ein CVCA Link-Zertifikat[26] erzeugt werden.
- Das zugehörige **CVCA Link-Zertifikat** MUSS vom noch aktiven privaten Root-Schlüssel signiert werden.
- Das initiale CVCA-Zertifikat und die nachfolgenden CVCA Link-Zertifikate MÜSSEN dem Ausweisproduzenten von der CVCA-eID als Vertrauensanker für die Ausweisproduktion übergeben werden. Dabei MÜSSEN die Authentizität und Integrität der Zertifikate durch die CVCA-eID abgesichert und durch den Ausweisproduzenten bei Empfang des jeweiligen Zertifikats sorgfältig geprüft werden.

4.4.1.2 Beantragungszeiten

Für die Beantragung eines Folgezertifikats MÜSSEN die im Folgenden festgelegten Reaktionsfristen der jeweiligen Zertifizierungsinstanz berücksichtigt werden, so dass das neue Zertifikat vor Ablauf des vorhergehenden Zertifikats ausgestellt werden kann.

Mit Reaktionsfrist ist hier der Zeitraum nach Eingang bis zur Beantwortung des Zertifikatsrequests zu verstehen. Diese Beantwortung besteht:

- im Regelfall in der Zusendung des beantragten Zertifikats, wenn dem nichts entgegensteht;
- in einer Begründung für die Nicht-Erstellung des Zertifikats, welche auch automatisch über entsprechende Fehlermeldungen des Kommunikationsprotokolls gemäß [TR-03129] erfolgen kann.

Das ausgestellte Zertifikat wird dem Antragssteller im Regelfall über die in [TR-03129] definierten Kommunikationsprotokolle zur Verfügung gestellt. Sollte dies aus technischen Gründen nicht möglich sein, wird auf die sekundäre Kommunikationsschnittstelle (siehe Kapitel 1.4.5) zurückgegriffen.

Beantragung von Zertifikaten bei der CVCA (DV-Zertifikate)

Die **Reaktionsfrist** zur Bearbeitung von Zertifikatsrequests eines DV durch die CVCA-eID beträgt **drei Arbeitstage**[27], wenn für die Beantragung und die Versendung des Zertifikats die Kommunikationsschnittelle gemäß [TR-03129] verwendet wird.

Beantragung von Zertifikaten bei einem DV (Terminal-Zertifikate)

Die **Reaktionsfrist** zur Bearbeitung von Zertifikatsrequests eines Terminals durch einen DV ist

- **drei Werktage** bei initialen Zertifikatsrequests ohne äußere Signatur
- **unverzüglich** bei initialen Zertifikatsrequests mit äußerer Signatur und Wiederholungsanträgen.

4.4.2 Beantragung von MDS-Zertifikaten

Jeder, der einen MDS Zertifikatsrequest stellen möchte, MUSS den Registrierungsprozess (Kapitel 3.2 „Registrierung“) erfolgreich durchlaufen haben.

Genereller Beantragungsprozess

Im Folgenden wird der Beantragungsprozess von MDS SubCA-Zertifikaten und Metadaten Signern beschrieben und die dabei zu beachtenden Vorgaben für **Zertifikatsnehmer** und **Zertifizierungsinstanz** werden festgelegt:

26 Für das initiale Root-Schlüsselpaar wird kein CVCA Link-Zertifikat erstellt.

27 Arbeitstage sind die Wochentage Montag bis Freitag, ausgenommen in Deutschland und/oder Nordrhein-Westfalen gesetzliche Feiertage sowie Rosenmontag, der 24.12. und der 31.12.

1. Generieren des Schlüsselpaares:
   1.1. Der **Zertifikatsnehmer** MUSS ein Schlüsselpaar gemäß [eIDAS-Crypto] generieren und MUSS dabei die Anforderungen aus den Kapiteln 5 „Sicherheitsmaßnahmen“ und 6 „Sicherheitsmaßnahmen für Schlüsselpaare“ berücksichtigen.
2. Generieren des Zertifikatsrequests:
   2.1. Der **Zertifikatsnehmer** generiert einen Zertifikatsrequest, welcher den neuen öffentlichen Schlüssel und eine innere Signatur auf Basis des zugehörigen privaten Schlüssels beinhalten MUSS. Die Erstellung des Zertifikatsrequests MUSS unter Berücksichtigung der Vorgaben aus Kapitel 3.1 „Namensgebung“ sowie [eIDAS-Crypto] und [RFC2986] erfolgen.
3. Zertifikatsrequest übermitteln:
   3.1. Der Zertifikatsrequest MUSS durch den **Zertifikatsnehmer** in einer Form übermittelt werden, die die Prüfung der Authentizität und Integrität des Zertifikatsrequests ermöglicht. Dabei KANN auf Terminalebene für den Request die Kommunikationsschnittelle aus Kapitel 1.4.5 „Kommunikation zwischen den Teilnehmern“ verwendet werden.
4. Zertifikatsrequest prüfen:
   4.1. Die **Zertifizierungsinstanz** MUSS sorgfältig prüfen, ob die Authentizität und Integrität des Zertifikatsrequests unverfälscht sind und der Zertifikatsrequest konform zu den Vorgaben aus 3.1 „Namensgebung“ sowie [eIDAS-Crypto] und [RFC2986] ist.
5. Registrierungsstatus prüfen:
   5.1. Die **Zertifizierungsinstanz** MUSS prüfen, ob der Zertifikatsnehmer aktuell berechtigt ist, Zertifikate zu erhalten und ob die Registrierungsinformationen über den Zertifikatsnehmer aktuell sind.
6. Zertifikat ausstellen:
   6.1. Die **Zertifizierungsinstanz** DARF KEIN Zertifikat auf Basis des Zertifikatsrequests ausstellen, wenn der vorherige Schritt zu einem negativen Ergebnis geführt hat. In diesem Fall MUSS die Zertifizierungsinstanz den Zertifikatsrequest ablehnen.
7. Antwort übermitteln:
   7.1. Die **Zertifizierungsinstanz** MUSS den Zertifikatsrequest beantworten und MUSS dabei die Vorgaben aus Kapitel 1.4.5 „Kommunikation zwischen den Teilnehmern“ einhalten. Die Antwort enthält entweder das Zertifikat oder die Ablehnung des Zertifikatsrequests.
8. Zertifikat annehmen:
   8.1. Der **Zertifikatsnehmer** MUSS das erhaltene Zertifikat in sein Zertifikatsverwaltungssystem unter Berücksichtigung der Vorgaben von Kapitel 2.1 „Zertifikatsverzeichnisse“ integrieren.
9. Löschen des alten Schlüssels:
   9.1. Wenn das neue Zertifikat erfolgreich in das Zertifikatsverwaltungssystem des Zertifikatsnehmers integriert werden konnte und der zugehörige private Schlüssel aktiviert wird (siehe Kapitel 6, „Sicherheitsmaßnahmen für Schlüsselpaare“), MUSS dieser den privaten Schlüssel des Vorgängerzertifikats unter Berücksichtigung der Vorgaben aus Kapitel 6, „Sicherheitsmaßnahmen für Schlüsselpaare“ löschen.
   9.2. Andernfalls muss ein neuer Zertifikatsrequest generiert und sämtliche Schritte zur Beantragung erneut durchlaufen werden.

Die beschriebenen manuellen Schritte SOLLEN auf Basis des 4-Augenprinzips durchgeführt werden.

4.5 Annahme von Zertifikaten (CV- und MDS-Zertifikate)

Bei Erhalt eines von ihm beantragten Zertifikats MUSS der Zertifikatsnehmer die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Weist der Zertifikatsnehmer das Zertifikat nicht zurück, gilt das Zertifikat als angenommen.

Um ein Zertifikat zurückzuweisen, MUSS der Zertifikatsnehmer eine Nachricht an die Zertifizierungsstelle schicken. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei feh-

lerhaften Zertifikaten SOLLTEN, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge benannt werden.

Im Normalfall erfolgt die Zurückweisung eines Zertifikats über die vorgegebenen Antworten innerhalb der Kommunikation gemäß [TR-03129]. Alternativ oder zusätzlich DARF eine Zurückweisung auf dem alternativen Kommunikationskanal (siehe Kapitel 1.4.5 „Kommunikation zwischen den Teilnehmern“) erfolgen.

Der Zertifikatsnehmer MUSS für Rückfragen der Zertifizierungsstelle zur Verfügung stehen. Hierfür SOLLTEN die Kontaktdaten aus der entsprechenden Registrierung genutzt werden.

4.6 Verwendung von Schlüsselpaar und Zertifikat

4.6.1 Verwendung von CV-Schlüsselpaar und CV-Zertifikat

Die innerhalb der CVCA-eID PKI erzeugten Zertifikate und Schlüssel DÜRFEN NICHT zu einem anderen Zweck verwendet werden, als den folgenden:

- **Nur CVCA bzw. CVCA Link-Zertifikat:** als Vertrauensanker der CVCA-eID PKI und zur Speicherung des zugehörigen öffentlichen Schlüssels als Vertrauensanker gemäß [TR-03110] im eID-Dokument oder
- zum Nachweis der Berechtigung[28] zum Zugriff auf bestimmte Datengruppen oder Funktionen der eID-Anwendung in hoheitlichen Dokumenten oder
- zur Erzeugung und Prüfung von Zertifikaten und Zertifikatsrequests innerhalb dieser PKI.

4.6.2 Verwendung von MDS Schlüsselpaar und MDS Zertifikat

Die MDS-Zertifikate und Schlüssel DÜRFEN NICHT zu einem anderen Zweck verwendet werden, als den folgenden:

- **nur Metadaten-Signer:** zum Signieren der Metadaten des entsprechenden Diensteanbieters[29] gemäß [eIDAS-Crypto];
- **alle Zertifikate:** zur Erzeugung und Prüfung von Zertifikaten und Zertifikatsrequests von MDS-Zertifikaten.

4.7 Gültigkeitszeiträume von Zertifikaten und Schlüsselpaaren

4.7.1 Gültigkeitszeiträume von CV-Zertifikaten und -Schlüsseln

In diesem Abschnitt werden die Gültigkeitszeiträume der Zertifikate und zugehörigen Schlüssel der CVCA-eID PKI definiert.

Der Gültigkeitszeitraum des privaten Schlüssels entspricht dem Gültigkeitszeitraum des zugehörigen Zertifikats. Der Gültigkeitszeitraum wird durch die ausstellende CA mit Hilfe der folgenden Felder gemäß [TR-03110] im Zertifikat festgeschrieben:

- „Certificate Effective Date” = Erster Tag der Gültigkeit (Datum der Zertifikatsgenerierung)
- „Certificate Expiration Date” = Letzter Tag der Gültigkeit[30]

Dabei dürfen die im Folgenden festgelegten maximalen Gültigkeitszeiträume nicht überschritten werden:

28 direkt oder als Teil der benötigten Zertifikatskette

29 d.h. des Diensteanbieters für den das Metadaten Signer DA-Zertifikat ausgestellt wurde

30 d.h., wenn gilt Certificate Effective Date = Certificate Expiration Date, dann ist das Zertifikat einen Tag bzw. 24 Stunden lang gültig.

CVCA- und DV-Ebene

Die maximalen Gültigkeitszeiträume auf CVCA- und DV-Ebene sind für den hoheitlichen und nicht hoheitlichen Bereich identisch und werden in der folgenden Tabelle dargestellt.

PKI-Ebene	Gültigkeitszeitraum
CVCA-eID	3 Jahre
DV	90 Tage

Tabelle 6: Gültigkeitszeiträume Zertifikate CVCA und DV

Im Standardfall werden die maximalen Gültigkeitszeiträume gesetzt, die CVCA-eID darf in Einzelfällen davon abweichen.

Die CVCA-eID und die Document Verifier SOLLEN darauf achten, rechtzeitig vor Ablauf ihrer Zertifikate ein neues Zertifikat zu beantragen, damit diese über die gesamte Betriebszeit Zertifikate mit dem vollen Gültigkeitszeitraum für ihre Zertifikatsnehmer ausstellen können.

Weitere Informationen zum Zeitmanagement von Zertifikaten sind in [TR-03110] enthalten.

Terminal-Ebene

Auf Terminal-Ebene sind die Gültigkeitszeiträume von Zertifikaten je nach Verwendungszweck und Betriebsart der Terminals unterschiedlich. Die verschiedenen Terminal-Typen werden in Abschnitt 1.2 beschrieben.

Hier setzt sich der Gültigkeitsraum aus einer Addition von Nutzungs- und Überlappungszeitraum zusammen, die wie folgt definiert sind:

- **Nutzungszeitraum:** In diesem Zeitraum darf das Zertifikat zur eID-Authentisierung oder zur Generierung von Wiederholungsanträgen verwendet werden. Der Zeitraum der Nutzung beginnt mit dem Tag der Ausstellung des Zertifikats.
- **Überlappungszeitraum:** Zeitraum zur Beantragung eines neuen Zertifikats. Das aktuelle Zertifikat kann innerhalb dieses Zeitraumes noch zur Authentisierung verwendet werden.

Hoheitlicher Bereich

Terminal	Anwendung	Betriebsart	Gültigkeitszeitraum (Nutzung + Überlappung)
Visualisierung / Änderungsterminal	Auskunftsbegehren / Änderungsdienst	verteilt	32 Tage (30+2)
Visualisierung / Änderungsterminal EAC-Box	Auskunftsbegehren / Änderungsdienst	integriert	2 Tage (1+1)
Terminals hoheitlicher Online-Dienste	PIN-Rücksetzdienst, Ummelde-/Schreibdienst	verteilt	2 Tage (1+1)

Tabelle 7: Gültigkeitszeiträume Zertifikate hoheitliche Terminals

Nicht hoheitlicher Bereich

Terminal	Anwendung	Gültigkeitszeitraum (Nutzung + Überlappung)
Elektronischer Identitätsnachweis		
Diensteanbieter	Lesen Datengruppen	2 Tage (1+1)
Diensteanbieter	Verifizieren von Alter / Wohnort	32 Tage (30+2)
Diensteanbieter	Nachladen QES	32 Tage (30+2)
Offline Terminal/Automatenbetrieb	Altersverifikation	37 Tage (30+7)
Offline Terminal/Automatenbetrieb	Lesen Datengruppen	In Abstimmung mit der CVCA-eID
Vor-Ort-Auslesen		
Diensteanbieter	Lesen von Datengruppen	2 Tage (1+1)

Tabelle 8: Gültigkeitszeiträume Zertifikate nicht-hoheitliche Terminals

4.7.2 Gültigkeitszeiträume von MDS-Zertifikaten und -Schlüsseln

Die maximalen Gültigkeitszeiträume und die Nutzungszeiträume der MDS-Zertifikate werden in der folgenden Tabelle festgelegt.

Ablauf des Nutzungszeitraumes bedeutet, dass der private Schlüssel des Zertifikats nicht mehr zum signieren verwendet werden darf, auch wenn der Gültigkeitszeitraum noch nicht abgelaufen ist. Zum Ablauf des Nutzungszeitraumes MUSS ein neues Schlüsselpaar generiert werden und ein neuer Zertifikatsantrag gestellt werden.

Die CVCA-eID teilt den DVs 90 Tage vor Ablauf des Nutzungszeitraums den exakten Termin der Ausstellung ihres Folgezertifikats mit.

Metadaten Signer DA-Zertifikate DÜRFEN NICHT länger gültig sein, als die durch die VfB ausgestellte Berechtigung des Diensteanbieters.

Zertifikatstyp	Gültigkeitszeitraum	Nutzungszeitraum
Metadaten Signer Root-Zertifikat	6 Jahre	3 Jahre
Metadaten Signer SubCA-Zertifikat	6 Jahre	3 Jahre
Metadaten Signer DA-Zertifikat	3 Jahre	3 Jahre

Tabelle 9: Gültigkeitszeiträume MDS-Zertifikate

4.8 Auslaufen von Berechtigungen

Berechtigungen von nicht-hoheitlichen Terminals werden von der VfB erteilt und haben eine begrenzte Gültigkeit. Im Falle eines bevorstehenden Auslaufens einer bestehenden Berechtigung eines nicht-hoheitlichen Diensteanbieter MUSS der nicht-hoheitliche DV, bei dem das Terminal des Diensteanbieters registriert ist, den Diensteanbieter mindestens 2 Monate vor Auslaufen der Berechtigung über diesem Umstand informieren.

4.9 Test-Systeme

Test-System

Das Test-System der CVCA-eID dient vor allem zur Durchführung der in Kapitel 3.2.1 geforderten Tests im Rahmen der Registrierung von Document Verifiern.

Zusätzlich bietet die CVCA-eID mit ihrem Test-System die Möglichkeit, DV-Zertifikate zu Testzwecken zu erhalten.

Außerdem werden technische Änderungen der CVCA-eID zunächst im Test-System durchgeführt. Die angeschlossenen DVs erhalten dadurch die Möglichkeit, die Änderungen vorzeitig zu erproben.

Die Teilnahme am Test-System kann über die Adresse cvca-eid@bsi.bund.de beantragt werden. Grundsätzlich erfordert die Teilnahme am Test-System eine Anbindung über eine Kommunikationsschnittelle gemäß [TR-03129]. Die CVCA-eID entscheidet über Ausnahmen.

Die im Wirk-System registrierten DVs MÜSSEN zusätzlich dauerhaft am Test-System teilnehmen und ihren Kunden entsprechend die Teilnahme ermöglichen.

Im Test-System gibt es keine festgelegten Reaktionsfristen für die Ausstellung von Zertifikaten.

Beta-System

Zusätzlich zum Test-System wird das Beta-System betrieben. Das Beta-System dient zur Erprobung von technischen Änderungen an der CVCA-eID PKI, *bevor* entschieden wird, ob diese zukünftig in das Wirk-System übernommen werden sollen.

Die Teilnahme am Beta-System kann über die Adresse cvca-eid@bsi.bund.de beantragt werden. Grundsätzlich erfordert die Teilnahme am Beta-System eine Anbindung über eine Kommunikationsschnittelle gemäß [TR-03129]. Die CVCA-eID entscheidet über Ausnahmen.

5 Sicherheitsmaßnahmen

Generell MÜSSEN die CVCA-eID, alle DVs und alle Terminalbetreiber ein Sicherheitskonzept erstellen, welches zumindest das folgende umfasst:

- **Nur CVCA und DVs:** Auflistung und Beschreibung aller IT Systeme, die Teil der Zertifizierungsinstanz, Registrierungsinstanz oder Kommunikationsschnittelle zu DV bzw. CVCA und Terminals sind;
- **Nur Terminals:** Auflistung und Beschreibung aller IT Systeme, die Teil des eID-Server oder des eID-Services sind inklusive der Kommunikationsschnittellen zwischen eID-Server, eID-Services und DV;
- Beschreibung aller Prozesse, die Teil der Aufgaben der CVCA, des DV oder des Terminals sind;
- Beschreibung der benötigten Rollen, Personal, Rollentrennung und Vertreterregelung;
- Beschreibung der Sicherheitsmaßnahmen für die o.g. Systeme inklusive des Notfall-Managements;
- Beschreibung der Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit des privaten Schlüssels;

Auf Anfrage der CVCA MÜSSEN die Sicherheitskonzepte der DVs und der Terminalbetreiber der CVCA durch die DVs[31] vorgelegt werden.

Die Sicherheitsmaßnahmen in den nachfolgenden Kapiteln MÜSSEN von

- der **CVCA-eID** sowie
- den **Document Verifiern** (hoheitliche DVs, BerCAs)

der CVCA-eID PKI realisiert werden.

Es wird EMPFOHLEN, dass **Diensteanbieter** und **hoheitliche Terminalbetreibe**r ein entsprechendes Sicherheitsniveau angelehnt an die beschriebenen Anforderungen gewährleisten.

Alle Anforderungen aus Kapitel 5 MÜSSEN auch für das Ausstellen, Verwalten und Nutzen von MDS-Zertifikaten eingehalten werden.

5.1 Systemsicherheit

Zur Herstellung und Aufrechterhaltung der Systemsicherheit MÜSSEN die **CVCA** und die **DVs** alle Anforderungen aus [TR-03145-1] Kapitel 6.3 bis Kapitel 6.15 und [TR-03145-4] erfüllen[32]. Diese behandeln u.a.:

- Notfall-Management und Behandlung von Vorfällen
- Prozessorganisation
- Angemessene kryptografische Maßnahmen
- Sichere Verwendung und Speicherung von Schlüsselmaterial
- Rollenmanagement
- Vertrauenswürdiges Personal
- Gesicherte IT Systeme und Netzwerke
- Physikalische Sicherheit
- Verfügbarkeit der Systeme
- Beendigung der Teilnahme
- Anforderungen an Dienstleister

5.1.1 Sicherheitsbereich

Ein Sicherheitsbereich im Sinne dieser CP ist ein klar räumlich abgetrennter Bereich inklusive der für den Betrieb eines IT-Systems notwendigen Hardware, Software, ggf. Netzanbindungen, des eingesetzten Perso-

31 Die Sicherheitskonzepte sind gemäß Kapitel 3.2.3.1 Teil der Registrierungsunterlagen der Terminalbetreiber beim DV.

32 Das BSI DARF für einzelne Anforderungen Ausnahmen genehmigen.

nals und der organisatorischen Maßnahmen. Der Zutritt zum Sicherheitsbereich MUSS auf das für die Aufrechterhaltung des Betriebs notwendige Personal beschränkt sein. Der Sicherheitsbereich MUSS nach [ISO/IEC 27001] zertifiziert sein. Die Zertifizierung MUSS den Betrieb der Komponente, für die der Sicherheitsbereich im CP CVCA-eID gefordert wird, umfassen.

5.2 Notfall-Management

In diesem Abschnitt werden zusätzliche Anforderungen an das Notfall-Management definiert.

5.2.1 Sperrung von Antragstellern

Das Sperren von CV-Zertifikaten über eine Sperrliste ist in der CVCA-eID PKI nicht vorgesehen.

Jede PKI-Instanz, die CV-Zertifikate ausstellt, MUSS Antragsteller sperren können (bspw. über eine interne Sperrliste). Für einen gesperrten Antragsteller DÜRFEN KEINE Zertifikate (weder CV- noch MDS-Zertifikate) ausgestellt werden.

5.2.2 Sperrung von MDS-Zertifikaten

MDS-Zertifikate werden über Certificate Revocation Lists (CRLs) zurückgerufen.

Die CVCA-eID MUSS eine CRL gemäß [RFC5280] für die Metadaten Signer SubCA-Zertifikate erstellen und veröffentlichen. Die CVCA-eID MUSS diese CRL zumindest alle 90 Tage erneuern. Zudem MUSS die CVCA-eID die CRL erneuern, wenn ein neuer Eintrag für die CRL hinzukommt.

Jeder kommerzielle DV MUSS eine CRL gemäß [RFC5280] für die Metadaten Signer DA-Zertifikate erstellen und veröffentlichen. Jeder DV MUSS seine CRL täglich erneuern.

Sperrgründe

Tritt eines der folgenden Ereignisse ein, so MUSS das entsprechende MDS-Zertifikat von der ausstellenden CA gesperrt und auf die entsprechende CRL gesetzt werden:

- mögliche Kompromittierung des zugehörigen privaten Schlüssels;
- Beendigung der Teilnahme des Zertifikatsnehmers an der CVCA-eID PKI;
- Auslaufen der Berechtigung durch die VfB für den Diensteanbieter, welcher „Subject“ des Zertifikats ist;
- Die mit dem Zertifikat signierten Metadaten sind nicht korrekt.
- Der Diensteanbieter wechselt den DV.
- Bei ausgelagertem Betrieb des eID-Servers: Der Diensteanbieter wechselt den Betreiber seines eID-Servers.

Veröffentlichung der CRLs

Die CVCA-eID und jeder DV MUSS die eigenen CRLs unter den, in den selbst ausgestellten Zertifikaten angegebenen, CRL Distribution Points veröffentlichen.

5.2.3 Vorgehensweise bei Kompromittierung oder anderen Vorfällen

Als **Vorfall** wird jegliches erfolgreiches Umgehen von Sicherheitsmaßnahmen, unbefugter Zugriff auf sensible Daten oder der Missbrauch des privaten Schlüssels definiert. Sensible Daten sind sowohl private Schlüssel als auch Registrierungseinträge und Registrierungsdaten sowie nicht-öffentliche Informationen über Infrastruktur, Konfiguration und Organisation des Gesamtsystems.

Die nachfolgend beschriebenen Prozesse MÜSSEN bei einem Vorfall oder einem Verdacht auf solchen eingehalten werden:

1. Eindämmung des Vorfalls durch geeignete Gegenmaßnahmen, wenn möglich Sicherung der Logdaten;
   1.1. Bei möglicher Kompromittierung des privaten Schlüssels MUSS die Verwendung desselben unverzüglich eingestellt werden.

2. Unverzügliche Meldung des Vorfalls an die übergeordnete Zertifizierungsinstanz;
3. Protokollierung und Analyse des Vorfalls;
4. Überarbeitung des Sicherheitskonzepts und daraus resultierende Anpassung der Sicherheitsmaßnahmen.
5. Zeigt der Vorfall einen sicherheitskritischen Mangel auf, ist eine sorgfältige Prüfung des Vorfalls erforderlich. Die Beseitigung des Mangels MUSS nachgewiesen werden, bevor ein neues Zertifikat ausgestellt werden darf.
6. Ist der Vorfall nicht sicherheitskritisch, kann ein erneuter initialer Zertifikatsrequest über die bestehende sichere TLS-Verbindung zugestellt werden, es MUSS zusätzlich der Fingerprint des Zertifikatsrequests über einen zweiten Kanal übermittelt werden (siehe Kapitel 4.2.1).
7. Bei einem schwerwiegenden Vorfall SOLLTE ein neues Zertifikat verweigert werden, bis die Behebung des Mangels durch einen Dritten (vgl. Kapitel 7 „Audits“) bestätigt wurde.

Vorfall auf Root-Ebene

Besteht Verdacht auf Kompromittierung oder Missbrauch ihres privaten Schlüssels, MUSS die CVCA-eID den Vorfall sorgfältig aufklären. Ein entsprechender Bericht über den Vorfall MUSS erstellt werden. Ist die Integrität des privaten Schlüssels nicht mehr gegeben, MUSS unverzüglich auf ein neues initiales CVCA Schlüsselpaar gewechselt werden. Das alte Schlüsselpaar DARF NICHT mehr verwendet werden. Alle Document Verifier MÜSSEN hierüber informiert werden. Zusätzlich MUSS der Schlüsselwechsel auf der CVCA-eID Webseite veröffentlicht werden.

Vorfall auf DV-Ebene

Besteht ein Verdacht auf einen Vorfall bei einem DV, MUSS dieser unverzüglich das Lagezentrum des BSI unter der Adresse Meldungen-eID@bsi.bund.de sowie die CVCA-eID unter der Adresse cvca-eid@bsi.bund.de per e-Mail informieren. Auch die Nichtverfügbarkeit der DV Dienste gilt als protokollierungs- und meldepflichtiger Vorfall. Handelt es sich beim DV um eine BerCA, MUSS gleichzeitig die VfB in Kenntnis gesetzt werden.

Zur Klärung des Vorfalls und der weiteren Vorgehensweise MUSS der DV der CVCA-eID folgende Unterlagen bereitstellen:

- Bericht über den Vorfall,
- Protokolldaten,
- in Relation stehende Betriebsdokumente.

Vorfall auf Terminal-Ebene

Besteht Verdacht auf einen Vorfall bei einem Terminal, MUSS der Terminalbetreiber unverzüglich den zuständigen DV informieren. Der DV MUSS dies wiederum unverzüglich an die CVCA-eID weitergeben. Handelt es sich um einen nicht-hoheitlichen Terminalbetreiber, MUSS gleichzeitig die VfB informiert werden.

Zur Klärung des Vorfalls und der weiteren Vorgehensweise MUSS der Terminalbetreiber dem DV folgende Unterlagen bereitstellen:

- Bericht über den Vorfall,
- Protokolldaten,
- in Relation stehende Betriebsdokumente.

Die entsprechenden Dokumente sind vom DV an die CVCA-eID weiterzugeben.

5.3 Auslagerung von IT-Systemen oder Aufgaben

Lässt die **CVCA, ein DV oder ein Terminalbetreiber** Teile oder die Gesamtheit ihrer Aufgaben oder IT-Systeme durch Auftragnehmer betreiben, MÜSSEN diese alle Sicherheitsanforderungen erfüllen, als ob ihr Auftraggeber selbst durchführen würde.

Zusätzlich MUSS sichergestellt werden, dass durch die Schnittstellen zwischen Auftraggeber und Auftragnehmer das Sicherheitsniveau der übertragenen Daten und der angeschlossenen Systeme nicht gefährdet wird.

5.4 Beendigung der Teilnahme

Bei Beendigung der Teilnahme an der CVCA-eID PKI MUSS **der Zertifikatsnehmer** die folgenden Pflichten erfüllen:

- der exakte Tag der Beendigung der Teilnahme MUSS festgelegt werden;
- die zuständige nächst-höhere PKI-Instanz MUSS vor Beantragung des vorletzten Zertifikats oder mindestens 30 Tage vor Beendigung der Teilnahme informiert werden.;
- alle privaten Schlüssel der PKI-Instanz MÜSSEN spätestens bei Einstellung des Betriebs sicher gelöscht werden. Dies bezieht sich sowohl auf die privaten Schlüssel aus der CVCA-eID PKI als auch auf die Kommunikationszertifikate (privater Schlüssel zu Client- und Server-Zertifikat);
- Ausgestellte bzw. erhaltene Zertifikate MÜSSEN entsprechend den Vorgaben aus Kapitel 2.1, „Zertifikatsverzeichnisse“ archiviert werden. Für denselben Zeitraum MUSS auch das Registrierungsverzeichnis archiviert werden.

Die **CA (CVCA-eID oder DV)**, welche den entsprechenden Zertifikatsnehmer registriert hat, MUSS die folgenden Regeln einhalten:

- die entsprechende Registrierung des Zertifikatsnehmers MUSS zur Beendigung der Teilnahme gesperrt werden;
- das letzte Zertifikat für den Teilnehmer MUSS so ausgestellt werden, dass es eine Gültigkeit bis einschließlich des Tages der Beendigung der Teilnahme NICHT überschreitet;
- die ausgestellten Zertifikate und Registrierungsinformationen MÜSSEN für den Zeitraum gemäß Kapitel 2.1, „Zertifikatsverzeichnisse“ archiviert werden;

Nach Beendigung der Teilnahme MUSS eine vollständige erneute Registrierung durchgeführt werden, wenn die Teilnahme wiederhergestellt werden soll.

5.4.1 Wechsel der BerCA

Plant ein Diensteanbieter die BerCA, von der er Zertifikate bezieht, zu wechseln, MUSS der Diensteanbieter:

- die VfB davon in Kenntnis setzen;
- sich bei der neuen BerCA unter Einhaltung der Vorgaben aus Kapitel 3.2.3 „Registrierung von Terminals“ vollständig neu registrieren;

Für die gegebenenfalls notwendige Migration des Terminal Sectors siehe Abschnitt 4.1.1.2.3.

6 Sicherheitsmaßnahmen für Schlüsselpaare

Die Teilnehmer der CVCA-eID PKI MÜSSEN für ihre Schlüsselpaare grundsätzlich die Anforderungen des Dokumentes [KeyLifecycle] erfüllen[33].

Die Sicherheitsmaßnahmen für Schlüsselpaare werden gemäß [KeyLifecycle] in die folgenden Sicherheitslevel unterteilt:

- **Sicherheitslevel 1**
- **Sicherheitslevel 2**

Die unterschiedlichen Anforderungen, die für das jeweilige Sicherheitslevel erfüllt werden müssen, sind in den folgenden Unterkapiteln definiert.

Werden die Anforderungen von **Sicherheitslevel 2** vollständig erfüllt, gilt dies implizit auch als Erfüllung von **Sicherheitslevel 1**[34].

Welche PKI-Teilnehmer welches Sicherheitslevel erfüllen müssen und welche Anforderungen zusätzlich zu denen gemäß [KeyLifecycle] gelten, wird in den folgenden Unterkapiteln dargelegt.

6.1 Sicherheitslevel der PKI-Teilnehmer

Die Sicherheitslevel MÜSSEN je nach PKI-Teilnehmer und Art des Schlüsselpaares wie folgt eingehalten werden:

- Die **CVCA-eID, der Sperrlistenbetreiber (eID-Sperrliste) und alle DVs** MÜSSEN für ihre Schlüsselpaare alle Anforderungen von **Sicherheitslevel 2** erfüllen (dies gilt auch für die Schlüsselpaare der MDS-Zertifikate). Abweichend davon:
  - **nicht-hoheitliche DVs:** Die Schlüsselpaare der **Sperrlisten für eID-Dokumente** MÜSSEN mindestens nach den Anforderungen des **Sicherheitslevels 1** geschützt werden.**Terminals** MÜSSEN grundsätzlich für ihre Schlüsselpaare alle Anforderungen von **Sicherheitslevel 1** erfüllen. Abweichend davon:
  - MÜSSEN Terminalbetreiber, die Terminals für **mehrere Diensteanbieter** betreiben, für die von Ihnen verwalteten und genutzten Schlüsselpaare die Anforderungen des **Sicherheitslevels 2** erfüllen.
  - MÜSSEN Terminalbetreiber von **hoheitlichen Terminals**, für die von Ihnen verwalteten und genutzten Schlüsselpaare die Anforderungen des **Sicherheitslevels 2** erfüllen.

6.2 Zusätzliche Anforderungen

Erzeugung von Schlüsselpaaren

Sicherheitslevel 1 und Sicherheitslevel 2: Zur Erzeugung der Schlüsselpaare MÜSSEN die kryptografischen Algorithmen und Schlüssellängen gemäß [TR-03116-2] eingesetzt werden.

Sicherung des privaten Schlüssels

Sicherheitslevel 2: Der Betrieb des Kryptografiemoduls MUSS in einem Sicherheitsbereich entsprechend Kapitel 5.1.1 erfolgen.

33 Das bedeutet, die Anforderungen des Dokumentes [KeyLifecycle] müssen erfüllt werden, aber die CVCA-eID DARF für einzelne Anforderungen Ausnahmen genehmigen.

34 Das bedeutet, ein Terminal, welches die Anforderungen von Sicherheitslevel 2 erfüllt, ist ebenfalls konform zur CP CVCA-eID.

Backup, Transfer und Wiederherstellung privater Schlüssel

Sicherheitslevel 1 und Sicherheitslevel 2: Die **CVCA** MUSS ein Backup ihres privaten Schlüssels durchführen und sicher speichern, um die Verlinkung der Vertrauensanker bzw. öffentlichen Schlüssel der CVCA-eID der eID-Dokumente durchgehend zu gewährleisten.

DVs und **Terminals** dürfen Backups für ihre privaten Schlüssel unter Einhaltung der unten stehenden Anforderungen entsprechend ihrem jeweiligen Sicherheitslevel durchführen. Dafür SOLLTE jedoch eine sorgfältige Abwägung zwischen Nutzen des Backups und Verringerung der Sicherheit der privaten Schlüssel durchgeführt werden.

6.3 Berechnung von Sperrlisten für eID-Dokumente

Bei der Berechnung der Sperrlisten für eID-Dokumente gemäß [TR-03129] durch die DV MÜSSEN zusätzlich zu den Anforderungen für den entsprechenden Sicherheitslevel die folgenden Regeln eingehalten werden:

- Es MUSS sichergestellt sein, dass die Vertraulichkeit der Sperrmerkmale jederzeit durch technische und organisatorische Maßnahmen gewährleistet ist.
- Die Erzeugung von Schlüsselpaaren MUSS in einem Sicherheitsbereich entsprechend Kapitel 5.1.1 erfolgen.
- Die dienstespezifischen Sperrlisten MÜSSEN auf Basis von [ITU-T X.690] DER-codiert erzeugt werden.
  Anmerkung: Dies ist eine Zusatzanforderung, welche die Vorgaben aus [TR-03129] verfeinert.

7 Audits

Jeder Betreiber einer PKI-Instanz der CVCA-eID PKI verpflichtet sich durch Antragstellung für eine Registrierung zur Einhaltung dieser von der Root (CVCA-eID) herausgegebenen CP zur Durchführung eines ordnungsgemäßen Betriebs.

CVCA-eID (Root-Ebene)

Die CVCA-eID MUSS alle drei Jahre eine Zertifizierung nach BSI [TR-03145-1] auf Basis eines entsprechenden Audits durch einen externen „Secure CA Operation"-Auditor für den Betrieb der CVCA-eID durchführen lassen. Dabei sind insbesondere auch die Anforderungen aus [TR-03145-4] zu beachten. Das BSI DARF für einzelne Anforderungen Ausnahmen genehmigen.

DV-Ebene

Jeder DV MUSS alle drei Jahre eine Zertifizierung nach BSI [TR-03145-1] auf Basis eines entsprechenden Audits durch einen externen „Secure CA Operation"-Auditor für den Betrieb des DV durchführen lassen. Dabei sind insbesondere auch die Anforderungen aus [TR-03145-4] zu beachten. Für kommerzielle DV MUSS dies auch die Erstellung und Verwaltung der MDS-Zertifikate beinhalten. Das BSI DARF für einzelne Anforderungen Ausnahmen genehmigen.

8 Anhang

8.1 Definitionen

Änderungsdienst
Hoheitlicher Funktionsumfang zur Aktualisierung der Angaben zur Adresse und im Rahmen des PIN-Managements.

Altersverifikation
In eID-Dokumenten verfügbare Funktionalität zum Nachweis einer geforderten Altersgrenze, ohne das tatsächliche Alter preiszugeben.

Antragssteller
Ein Zertifikatsnehmer, der einen Zertifikatsrequest stellt.

Auskunftsbegehren
Recht des Dokumenten-Inhabers zur Visualisierung der im Chip des eID-Dokuments gespeicherten, persönlichen Daten, vgl. [PAuswG].

Berechtigungszertifikateanbieter (BerCA)
Berechtigungszertifikateanbieter gemäß [PAuswV]. Hier auch Nicht-hoheitlicher Document Verifier.

Country Verifying Certification Authority
Wurzelinstanz der CVCA PKI (siehe Kapitel 1.4)

CVCA Zertifikat
Als CVCA Zertifikat bezeichnet man das selbst-signierte Zertifikat der CVCA zum Root-Schlüssel. Die Certification Authority Reference und die Certificate Holder Reference des CVCA Zertifikats sind identisch.

CVCA Link-Zertifikat
Ein CVCA Link-Zertifikat beinhaltet den öffentlichen Anteil des aktuellen Root-Schlüsselpaares als Public Key (öffentlichen Schlüssel), die Signatur des Zertifikats wurde jedoch mit dem privaten Schlüssel des Vorgänger-Root-Schlüsselpaares erzeugt. Die Certification Authority Reference und die Certificate Holder Reference unterscheiden sich in der Seriennummer.

Diensteanbieter
PKI-Teilnehmer auf Terminal-Ebene. Begriff gemäß § 2, Absatz 3 [PAuswG].

Document Verifier
Zertifikatsnehmer und Zertifizierungsinstanz der mittleren PKI-Ebene (siehe Kapitel 1.4).

eID-Anwendung
Funktionalität und Datenstruktur für Online-Identitätsnachweise mit dem elektronischen Personalausweis, der eID-Karte für Unionsbürger und dem elektronischen Aufenthaltstitel.

eID-Dokument
Innerhalb dieser Certificate Policy Oberbegriff für den elektronischen Personalausweis, den elektronischen Aufenthaltstitel, die eID-Karte für Unionsbürger sowie die Smart-eID zu verstehen.

Fingerprint
Hashwert über ein Zertifikat oder einen Zertifikatsrequest.

Identifizierungsdiensteanbieter
PKI-Teilnehmer auf Terminal-Ebene gemäß § 2, Absatz 3a [PAuswG].

Kryptografiemodul
Funktionseinheit zur Erzeugung, Verwaltung und sicheren Speicherung kryptografischen Schlüsselmaterials und Erstellung von elektronischer Signaturen.

Kommunikationszertifikate
Zertifikate zur Authentisierung innerhalb einer TLS-Verbindung zwischen den PKI-Teilnehmern (siehe Kapitel 1.4.5).

Metadaten Signer Zertifikate
Zertifikate im X.509 Format, welche zur Ermöglichung der Nutzung von eIDAS-Anwendungen gemäß eIDAS-Verordnung (siehe [eIDAS-VO]) entsprechend der [eIDAS-Inter] verwendet werden. Die MDS-Zertifikate werden außer von der CVCA-eID nur von den kommerziellen Instanzen der CVCA-eID PKI beantragt oder ausgestellt (siehe Kapitel 1.2.2).

Qualifizierte elektronische Signatur
Qualifizierte elektronische Signatur entsprechend dem Signaturgesetz (SigG).

Request-Signer-Zertifikat
Optionales Zertifikat zur Authentisierung von Zertifikatsanträgen.

Smart-eID
Hier verwendeter Begriff für „Elektronischer Identitätsnachweis mit einem mobilen Endgerät“

Sperrdienst
Zuständige Stelle für die Bereitstellung von Sperrlisten zu den von Ausweisinhabern ausgelösten eID-Sperren (siehe [TR-03127]).

Terminal
Ein Terminal ist ein Gerät oder Programm, das mit dem Chip im eID-Dokument kommuniziert.

Vergabestelle für Berechtigungszertifikate (VfB)
Für die Erteilung und Aufhebung von Berechtigungen nach §21 [PAuswG] zuständige Stelle.

Visualisierung
Anzeige der elektronisch auf dem Chip eines eID-Dokument gespeicherten dokumenten- und personenbezogenen Daten auf einem Lesegerät.

Vor-Ort-Diensteanbieter
PKI-Teilnehmer auf Terminal-Ebene für das Vor-Ort-Auslesen unter Anwesenden gemäß §18a [PAuswG].

Zertifikatsnehmer
Eine Instanz der PKI, die von einer übergeordneten Instanz Zertifikate bezieht (siehe Abschnitt 1.4.3). Ausnahme bildet die CVCA-eID, die sich selbst Zertifikate ausstellt.

Zertifikatsrequest
Der technische Antrag auf ein Zertifikat (siehe Certificate Request in [TR-03110]).

8.2 Abkürzungen

BerCA Certification Authority eines Berechtigungszertifikateanbieters
BSI Bundesamt für Sicherheit in der Informationstechnik
CA Certification Authority
CAR Certification Authority Reference
CHAT Certificate Holder Authorization Template
CHR Certificate Holder Reference

CPS Certificate Practise Statement
CRL Certificate Revocation List (Zertifikatssperrliste)
CVCA Country Verifying Certification Authority
DA Diensteanbieter
DG Datengruppe
DV Document Verifier
EAC Extended Access Control (siehe BSI TR-03110)
eID elektronischer Identitätsnachweis (Anwendung von eID-Dokumenten)
HSM Hardware Sicherheitsmodul
ISO International Organization for Standardization
MDS Metadaten Signer
OID Object Identifier
PKI Public Key Infrastructure
QES qualifizierte elektronische Signatur
RA Registration Authority
RFC Requests for Comments (Technischer Standard)
SPOC Single Point of Contact - Kommunikationsschnittstelle zur CVCA-eID
TLS Transport Layer Security (Protokoll Verbindungsauthentisierung/Verschlüsselung)
TR Technische Richtlinie
URL Uniform Resource Locator (hier Internetadresse)
VfB Vergabestelle für Berechtigungszertifikate

8.3 Literaturverzeichnis

AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (AufenthG)
AufenthV	Aufenthaltsverordnung
CP-Annex	BSI: Annex zur CP CVCA-eID - Vergaben für die Vergabe von Berechtigungszertifikaten an andere EU-Mitgliedsstaaten
eIDAS-Crypto	eIDAS - Cryptographic requirements for the Interoperability Framework TLS and SAML - https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10
eIDAS-Inter	eIDAS – Interoperability Architecture - https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10
eIDAS-SAML	eIDAS SAML Attribute Profile - https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10
eIDAS-VO	Das Europäische Parlament und der Rat der Europäischen Union: VERORDNUNG (EU) Nr. 910/2014 der Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32014R0910)
ISO/IEC 27001	ISO/IEC: ISO/IEC 27001:2013 'Information technology - Security techniques – Information security management systems - Requirements', ISO/IEC JTC1/SC27
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
KeyLifecycle	BSI: Key Lifecycle Security Requirements
PAuswG	Gesetz über den Personalausweis und den elektronischen Identitätsnachweis(Personalausweisgesetz)
PAuswV	Verordnung über Personalausweise, eID-Karten für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis (Personalausweisverordnung)
RFC2119	Bradner, S.: Key words for use in RFCs to indicate requirement levels
RFC2986	RSA Security: M. Nystrom, B. Kaliski: PKCS #10: Certification Request Syntax Specification
RFC5280	D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC6454	IETF, A. Barth: The Web Origin Concept
TR-03110	BSI: Technical Guideline TR-03110 - Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS-Token
TR-03116-2	BSI: Technische Richtlinie TR-03116-2 - Kryptografische Vorgaben für Projekte der Bundesregierung
TR-03116-4	BSI: Technische Richtlinie TR-03116-4 - Kryptografische Vorgaben für Projekte der Bundesregierung Teil 4 – Vorgaben für Kommunikationsverfahren im eGovernment
TR-03124-1	BSI: Technical Guideline TR-03124-1 eID-Client – Part 1: Specifications
TR-03127	BSI: Technische Richtlinie TR-03127 - eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control – Personalausweis, elektronischer Aufenthaltstitel und eID-Karte für Unionsbürger
TR-03129	BSI: Technical Guideline TR-03129 - PKI for the Extended Access Control (EAC), Protocol for the Management of Certificates and CRLs
TR-03130	BSI: Technical Guideline TR-03130 - eID-Server
TR-03131	BSI: Technical Guideline TR-03131 - EAC-Box Architecture and Interfaces

TR-03145-1 BSI: Technical Guideline 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'

TR-03145-4 BSI: Technical Guideline TR-03145-4 - Secure CA operation, Part 4 - Specific requirements for Authorization Certificate Authorities (BerCA) of the CVCA-eID PKI