



Bundesamt  
für Sicherheit in der  
Informationstechnik



Dokument ist noch aktuell. (Stand 2020)

## Certificate Policy für die ePass-Anwendung der hoheitlichen Dokumente

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel.: +49 22899 9582-0

E-Mail: [cvca-epass@bsi.bund.de](mailto:cvca-epass@bsi.bund.de)

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2010

## Inhaltsverzeichnis

1	Einleitung.....	7
1.1	Überblick.....	9
1.1.1	CVCA-ePass.....	9
1.1.2	Document Verifier.....	9
1.1.3	Inspektionssysteme.....	10
1.2	Name und Identifizierung des Dokuments.....	10
1.3	PKI-Teilnehmer.....	11
1.3.1	Zertifizierungsstellen.....	11
1.3.2	Registrierungsstellen.....	12
1.3.3	Zertifikatsnehmer.....	13
1.3.4	Zertifikatsnutzer.....	13
1.3.5	Andere Teilnehmer.....	14
1.4	Verwendung von Zertifikaten.....	14
1.4.1	Erlaubte Verwendung von Zertifikaten.....	14
1.4.2	Verbotene Verwendung von Zertifikaten.....	15
1.5	Administration der Policy.....	15
1.5.1	Pflege der Certificate Policy.....	15
1.5.2	Zuständigkeit für das Dokument.....	15
1.5.3	Ansprechpartner / Kontaktperson.....	15
1.5.4	Zuständiger für die Anerkennung eines CPS.....	15
1.5.5	CPS-Aufnahmeverfahren.....	15
2	Veröffentlichungen und Aufbewahrung.....	16
2.1	Verzeichnisse.....	16
2.2	Veröffentlichung von Informationen zur Zertifikatserstellung.....	16
2.2.1	CVCA-ePass.....	16
2.2.2	DV-Ebene.....	16
2.3	Zeitpunkt und Häufigkeit der Veröffentlichungen.....	17
2.4	Zugriffskontrollen auf Verzeichnisse.....	17
3	Identifizierung und Authentifizierung.....	18
3.1	Regeln für die Namensgebung.....	18
3.1.1	Arten von Namen.....	18
3.1.2	Notwendigkeit für aussagefähige Namen.....	20
3.1.3	Anonymität oder Pseudonymität von Zertifikatsnehmern.....	20
3.1.4	Interpretationsregeln für verschiedene Namensformen.....	20
3.1.5	Eindeutigkeit von Namen.....	20
3.1.6	Anerkennung, Authentifizierung und die Rolle von Markennamen.....	20
3.2	Initiale Überprüfung der Identität.....	21
3.2.1	Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels.....	21
3.2.2	Authentifizierung von Organisationszugehörigkeiten.....	21
3.2.3	Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers.....	23
3.2.4	Ungeprüfte Angaben zum Zertifikatsnehmer.....	23
3.2.5	Prüfung der Berechtigung zur Antragstellung.....	23
3.2.6	Kriterien für den Einsatz interoperierender Systeme/Einheiten.....	24
3.3	Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung.....	24
3.3.1	Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung.....	24
3.3.2	Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen.....	25

3.4	Identifizierung und Authentifizierung von Anträgen auf Sperrung.....	25
4	Betriebsanforderungen für den Lebenszyklus der Zertifikate.....	26
4.1	Zertifikatsantrag.....	26
4.1.1	Wer kann einen Zertifikatsantrag stellen?.....	26
4.1.2	Beantragungsprozess und Zuständigkeiten.....	27
4.2	Verarbeitung von Zertifikatsanträgen.....	29
4.2.1	Durchführung der Identifizierung und Authentifizierung.....	29
4.2.2	Annahme oder Ablehnung von Zertifikatsanträgen.....	30
4.2.3	Fristen für die Bearbeitung von Zertifikatsanträgen.....	30
4.3	Ausgabe von Zertifikaten.....	30
4.3.1	Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats.....	30
4.4	Annahme von Zertifikaten.....	31
4.4.1	Veröffentlichung von Zertifikaten durch die CA.....	31
4.5	Verwendung von Schlüsselpaar und Zertifikat.....	31
4.5.1	Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer.....	31
4.5.2	Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer.....	32
4.6	Zertifikatserneuerung.....	32
4.7	Zertifizierung nach Schlüsselerneuerung.....	32
4.7.1	Bedingungen der Zertifizierung nach Schlüsselerneuerungen.....	32
4.7.2	Wer darf Zertifikate für Schlüsselerneuerungen beantragen?.....	33
4.7.3	Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen.....	33
4.7.4	Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats.....	33
4.7.5	Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen.....	33
4.7.6	Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA.....	33
4.7.7	Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats.....	33
4.8	Änderungen am Zertifikat.....	33
4.9	Sperrung und Suspendierung von Zertifikaten.....	33
4.10	Service zur Statusabfrage von Zertifikaten.....	34
4.11	Beendigung der Teilnahme.....	34
4.12	Hinterlegung und Wiederherstellung von Schlüsseln.....	34
5	Organisatorische, betriebliche und physikalische Sicherheitsmaßnahmen.....	35
5.1	Physikalische Sicherheitsmaßnahmen.....	35
5.1.1	Generelle Sicherheitsmaßnahmen.....	35
5.1.2	Erweiterte Sicherheitsmaßnahmen.....	36
5.2	Verfahrensanweisungen.....	36
5.3	Personalkontrolle.....	36
5.4	Überwachungsmaßnahmen.....	36
5.5	Archivierung von Aufzeichnungen.....	37
5.6	Schlüsselwechsel einer Zertifizierungsstelle.....	37
5.7	Notfall-Management.....	38
5.7.1	Behandlung von Vorfällen und Kompromittierung.....	38
5.7.2	Kompromittierung des privaten Schlüssels einer CA.....	39
6	Technische Sicherheitsmaßnahmen.....	40
6.1	Erzeugung und Installation von Schlüsselpaaren.....	40
6.1.1	Erzeugung von Schlüsselpaaren.....	40
6.1.2	Lieferung privater Schlüssel an Zertifikatsnehmer.....	40
6.1.3	Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber.....	40
6.1.4	Lieferung öffentlicher Schlüssel der CA an Zertifikatsnutzer.....	41

6.1.5	Schlüssellängen und kryptografische Algorithmen.....	41
6.1.6	Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle.....	41
6.1.7	Verwendungszweck der Schlüssel.....	41
6.2	Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module.....	41
6.2.1	Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln.....	42
6.2.2	Hinterlegung privater Schlüssel.....	42
6.2.3	Backup privater Schlüssel.....	42
6.2.4	Archivierung privater Schlüssel.....	42
6.2.5	Transfer privater Schlüssel in oder aus kryptographischen Modulen.....	43
6.2.6	Speicherung privater Schlüssel in kryptographischen Modulen.....	43
6.2.7	Aktivierung privater Schlüssel.....	43
6.2.8	Deaktivierung privater Schlüssel.....	43
6.2.9	Zerstörung privater Schlüssel.....	43
6.2.10	Beurteilung kryptographischer Module.....	43
6.3	Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module.....	44
6.3.1	Archivierung öffentlicher Schlüssel.....	44
6.3.2	Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren.....	45
6.4	Aktivierungsdaten.....	46
6.5	Sicherheitsmaßnahmen für die Rechneranlagen.....	46
6.6	Zeitstempel.....	47
6.7	Validierungsmodell.....	47
7	Profile für Zertifikate und Sperrlisten.....	48
7.1	Profile für Zertifikate und Zertifikatsanträge.....	48
7.1.1	Zugriffsrechte.....	48
7.1.2	Zertifikatserweiterung.....	49
7.2	Profile für Sperrlisten.....	49
7.3	Profile für OCSP-Dienste.....	49
8	Überprüfung und andere Bewertungen.....	50
8.1	Inhalte, Häufigkeit und Methodik.....	50
8.2	Reaktionen auf identifizierte Vorfälle .....	51
9	Sonstige finanzielle und rechtliche Regelungen.....	53
9.1	Preise.....	53
9.2	Finanzielle Zuständigkeiten.....	53
10	Referenzen.....	54

## Abbildungsverzeichnis

Abbildung 1: Gesamtübersicht der CVCA-ePass PKI.....	12
--	----

## Tabellenverzeichnis

Tabelle 1: Identifikation des Dokuments.....	15
Tabelle 2: Übersicht der PKI-Teilnehmer.....	15
Tabelle 3: Zertifizierungsstellen der CVCA-ePass PKI.....	16

Tabelle 4: Registrierungsstellen (RAs) der CVCA-ePass PKI.....	17
Tabelle 5: Erlaubter Verwendungszweck von Zertifikaten und zugehöriger privater Schlüssel.....	18
Tabelle 6: Kontaktdaten.....	19
Tabelle 7: Certificate Holder Reference DV national-begrenzt.....	23
Tabelle 8: Certificate Holder Reference DV national.....	23
Tabelle 9: Zur Zertifikatsantragsstellung berechnete Organisationen.....	31
Tabelle 10: Fristen zur Bearbeitung von Zertifikatsanträgen.....	34
Tabelle 11: Archivierung öffentlicher Schlüssel.....	48
Tabelle 12: Setzen von Gültigkeitszeiträumen in CV-Zertifikaten der CVCA-ePass PKI.....	49
Tabelle 13: Gültigkeitszeiträume CVCA-ePass- und DV-Ebene.....	49
Tabelle 14: Gültigkeitszeiträume in Inspektionssystemen.....	50
Tabelle 15: Übersicht Felder CV-Zertifikat mit vorgegebener Wertebelegung.....	52
Tabelle 16: Erlaubte Zugriffsrechte für CVCA-/DV-Zertifikate.....	53
Tabelle 17: Prüfanforderungen Document Verifier.....	55
Tabelle 18: Prüfanforderungen Betreiber von Inspektionssystemen.....	55

# 1 Einleitung

Der elektronische Personalausweis, der elektronische Reisepass und der elektronische Aufenthaltstitel beinhalten einen elektronischen Chip mit der ePass-Anwendung, welche zur Identifikation des Ausweisinhabers und Prüfung der Echtheit des Dokuments dient. Diese Ausweisdokumente werden unter dem Begriff „**hoheitliche Dokumente**“ zusammengefasst.

Die elektronischen Chips der hoheitlichen Dokumente geben den Zugriff auf die gespeicherten Daten nur gegen Nachweis einer entsprechenden Berechtigung frei. Ob eine solche Berechtigung besteht und für welche Daten diese gilt, wird durch die Vergabe von elektronischen Zertifikaten über eine Public Key Infrastruktur (PKI) geregelt. Diese Zertifikate werden auch Berechtigungszertifikate genannt. Die Berechtigungszertifikate werden gemäß [TR-03110] erstellt und basieren auf der Struktur von CV-Zertifikaten (Card Verifiable).

Die Vergabe der Berechtigungszertifikate wird durch eine **Public Key Infrastruktur (PKI)** geregelt, deren Wurzelinstanz die **Country Verifying Certificate Authority** im Kontext der ePass-Anwendung (**CVCA-ePass**) ist. Diese PKI wird im Folgenden **CVCA-ePass PKI** genannt.

Die ePass-Anwendung der hoheitlichen Dokumente soll sowohl von nationalen Stellen wie den Kontrollbehörden oder den Ausweisbehörden als auch bei Kontrollbehörden anderer Nationen gelesen werden können.

Das vorliegende Dokument ist die **Certificate Policy (CP)**, welche die Regeln für die Teilnehmer der CVCA-ePass PKI definiert. Diese Regeln sind für die nationalen Teilnehmer der PKI bindend, um Berechtigungszertifikate aus der CVCA-ePass PKI erhalten zu können. Für Teilnehmer anderer Nationen werden lediglich Empfehlungen gemacht, diese Teilnehmer müssen die Einhaltung der CP aus den Entscheidungen der Kommission der Europäischen Gemeinschaften [K(2008)8657] und [K(2009)7476] nachweisen, um Berechtigungszertifikate von der CVCA-ePass PKI zu erhalten.

Inhaltliche Grundlagen für die Erstellung der Certificate Policy bilden insbesondere die folgenden Dokumente:

- Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI) - [TR-03110]
- EAC-PKI'n für den elektronischen Personalausweis [TR-03128]
- PKI for the Extended Access Control (EAC), Protocol for the Management of Certificates and CRLs [TR-03129]

Die Struktur dieses Dokuments orientiert sich an dem Request for Comments (RFC) 3647 [RFC 3647], um eine zweckdienliche Vergleichbarkeit mit anderen Policies zu unterstützen.

Die Schlüsselworte „MUSS“/„MÜSSEN“, „DARF NICHT“/„DÜRFEN NICHT“, „DARF KEIN“/„DÜRFEN KEIN“, „DARF KEINE“/„DÜRFEN KEINE“, „SOLL“/„SOLLEN“, „SOLL NICHT“/„SOLLEN NICHT“, „SOLLTE“/„SOLLTE“, „SOLLTE NICHT“/„SOLLTEN NICHT“, „EMPFOHLEN“ und „KANN“/„KÖNNEN“ in diesem Dokument sind wie in [RFC 2119] definiert zu interpretieren.

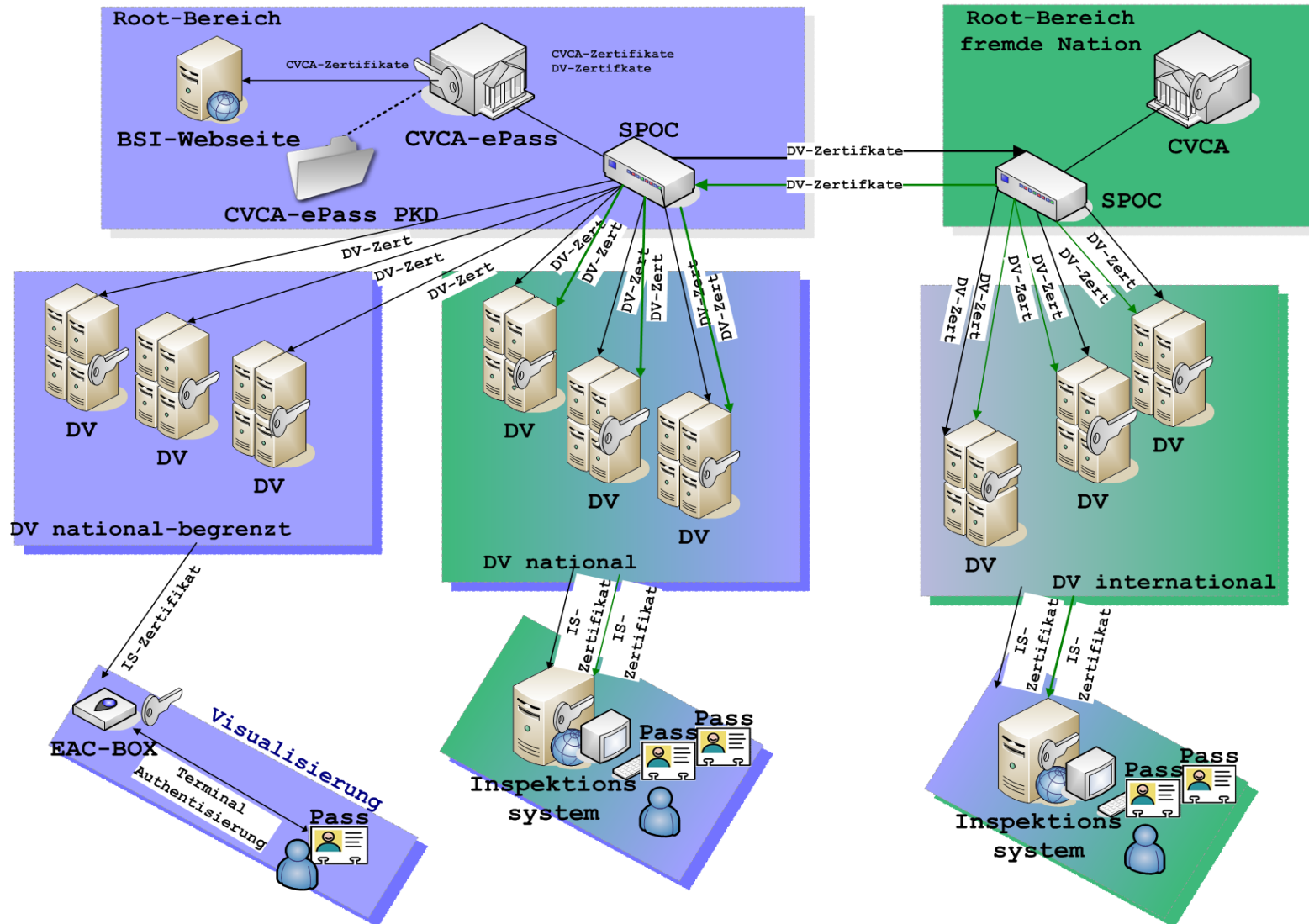


Abbildung 1: Gesamtübersicht der CVCA-ePass PKI



## 1.1 Überblick

Die CVCA-ePass PKI ist gemäß [TR-03110] grundsätzlich in drei Stufen unterteilt:

- die **CVCA-ePass**, bildet als nationaler Vertrauensanker die Root für den nationalen Bereich der CVCA-ePass PKI,
- die **Document Verifier (DV)** verwalten zusammengehörige Inspektionssysteme bzw. Lesegeräte,
- die **Inspektionssysteme (IS)** sind Lesegeräte, die für das Auslesen der in der ePass-Anwendung gespeicherten Daten eingesetzt werden, inklusive der weiteren Geräte und Infrastruktur, die für die Erzeugung und Verwaltung von Schlüsselpaaren und den Empfang von Zertifikaten vom zuständigen DV benötigt werden.

Im Folgenden werden die Instanzen der drei Stufen und ihre Aufgaben näher beschrieben und Abbildung 1 stellt die Zusammenhänge grafisch dar.

### 1.1.1 CVCA-ePass

Die CVCA-ePass stellt sowohl für nationale als auch für ausländische Document Verifier Zertifikate aus und berechtigt diese dadurch Berechtigungszertifikate für Inspektionssysteme auszustellen. Im Folgenden wird mit **CVCA-ePass** immer die deutsche CVCA für die ePass-Anwendung bezeichnet, ausländische CVCA die Zertifikate für die ePass-Anwendung ausstellten werden schlicht mit CVCA bezeichnet.

Des Weiteren berechtigt die CVCA-ePass nationale Document Verifier zur Beantragung von Zertifikaten bei einer ausländischen CVCA durch das Signieren der entsprechenden Zertifikatsanträge.

Zur Kommunikation mit den nationalen DV wird ein Single Point of Contact (**SPOC**) verwendet, dabei werden die Protokolle und Regelungen gemäß [TR-03129] eingesetzt. Die Kommunikation mit den ausländischen CVCA bzw. ausländischen DV findet zwischen dem nationalen SPOC und dem SPOC der ausländischen CVCA gemäß [CSN369791] statt.

Die CVCA-ePass betreibt mit dem **CVCA-ePass PKD** einen Verzeichnisdienst, in welchem alle von der CVCA-ePass ausgestellten Zertifikate und signierten Zertifikatsanträge archiviert werden. Alle zur CVCA-ePass gehörigen Systeme werden vom Bundesamt für Sicherheit in der Informationstechnik betrieben.

Die CVCA-ePass stellt Zertifikate aus, signiert Zertifikatsanträge der DV und archiviert diese Daten. Zusätzlich stellt die CVCA-ePass noch eigene selbst-signierte CVCA-Zertifikate und CVCA-Link-Zertifikate aus. Außerdem ist die CVCA-ePass verpflichtet, alle ihr vorgelegten Zertifikatsanträge gründlich zu prüfen, bevor eine Signatur erstellt wird.

Bei der Produktion der hoheitlichen Dokumente wird ein Wurzelzertifikat der CVCA-ePass PKI als Vertrauensanker in den RF-Chip des Dokuments eingebracht.

### 1.1.2 Document Verifier

Die Document Verifier vergeben Zertifikate an Inspektionssysteme und berechtigen diese damit zum Auslesen von Daten aus der ePass-Anwendung in hoheitlichen Dokumenten.

Eine detaillierte Beschreibung der von hoheitlichen Document Verifier zu erfüllenden Anforderungen ist in [TR-03128] zu finden.

Die Document Verifier werden in drei Gruppen unterteilt:

- Deutsche Document Verifier, welche die Berechtigung haben, sowohl bei der CVCA-ePass als auch bei anderen Nationen Zertifikate zu beantragen. Diese werden im Folgenden als **DV national** bezeichnet.
- Deutsche Document Verifier, die nur bei der CVCA-ePass Zertifikate beantragen dürfen. Diese werden im Folgenden als **DV national-begrenzt** bezeichnet.
- Ausländische Document Verifier, die über ihren SPOC bei der deutschen CVCA ePass Zertifikate beantragen dürfen. Diese werden im Folgenden als **DV international** bezeichnet.

**DV national** sind vor allem Kontrollbehörden mit der Aufgabe die Identität von Personen festzustellen. **DV national-begrenzt** vergeben Zertifikate für Inspektionssysteme nur im nationalen Bereich für die Qualitätssicherung von hoheitlichen Dokumenten bei ihrer Ausgabe und für Auskunftsbegehren des Bürgers.

**DV international** und DV national werden jeweils nur bei dem SPOC ihrer eigenen Nation registriert. Zertifikatsanträge an eine andere Nation werden über den SPOC der eigenen Nation gestellt. Dieser versendet anschließend auch das zum Zertifikatsantrag erstellte Zertifikat an den DV.

Neben dem Ausstellen von Zertifikaten für Inspektionssysteme und dem Archivieren dieser Daten, ist ein Document Verifier verpflichtet, alle ihm vorgelegten Zertifikatsanträge gründlich zu prüfen, bevor eine Signatur erstellt wird.

### 1.1.3 Inspektionssysteme

Inspektionssysteme erhalten ihre IS-Zertifikate für den Zugriff auf geschützte Daten auf dem RF-Chip der hoheitlichen Dokumente von den Document Verifiern. Inspektionssysteme stellen selbst keine Zertifikate aus.

Die Protokolle zum Nachweis der Berechtigung für den Zugriff auf Daten in den hoheitlichen Dokumenten sind in [TR-03110] definiert.

## 1.2 Name und Identifizierung des Dokuments

Dieses Dokument ist die Certificate Policy (CP) der deutschen Country Verifying Certificate Authority - electronic Passport (CVCA-ePass).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dieser CP folgenden Object Identifier (OID) zugeordnet: 0.4.0.127.0.7.3.1.1.2.1 .

Dieses Dokument kann unter <https://www.bsi.bund.de/cvca-ePass> bezogen werden.

<i>Identifikator</i>	<i>Wert</i>
<b>Titel</b>	Certificate Policy für die ePass-Anwendung der hoheitlichen Dokumente (CP CVCA-ePass)
<b>Version</b>	1.0
<b>OID</b>	0.4.0.127.0.7.3.1.1.2.1

Tabelle 1: Identifikation des Dokuments

### 1.3 PKI-Teilnehmer

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

<b>Instanz der PKI</b>	<b>Zertifizierungsstelle</b>	<b>Registrierungsstelle</b>	<b>Zertifikats-Neher</b>	<b>Zertifikats-Nutzer</b>
CVCA-ePass	■	■	■	■
DV	■	■	■	■
Inspektionssystem			■	■
Elektronisches Ausweisdokument				■

Tabelle 2: Übersicht der PKI-Teilnehmer

#### 1.3.1 Zertifizierungsstellen

Zertifizierungsstellen (Certification Authority, CA), welche die Anforderungen dieser Certificate Policy erfüllen, stellen Zertifikate für den Zugriff auf die ePass-Anwendung der hoheitlichen Dokumente aus.

Die **Country Verifying Certification Authority – electronic Passport (CVCA-ePass)** bildet den nationalen Vertrauensanker (Root) der CVCA-ePass PKI für die Berechtigung zum Zugriff auf die ePass-Funktion der hoheitlichen Dokumente. Folgende Zertifikate werden von der CVCA-ePass ausgestellt:

- selbst-signierte CVCA-Zertifikate ( $C_{CVCA}$ ),
- DV-Zertifikate ( $C_{DV}$ ) sowie
- CVCA-Link-Zertifikate (Link- $C_{CVCA}$ )
- Zusätzlich signiert die CVCA-ePass Zertifikatsanträge der DV national an fremde CVCA

Die **Document Verifying Certification Authority (DVCA)**, auch als **Document Verifier (DV)** bezeichnet, ist eine organisatorische Einheit, welche einen Verbund von Inspektionssystemen (IS) betreut, die als teilnehmende Inspektionssysteme eingestuft werden. Der DV ist von der CVCA-ePass zur Ausgabe von Berechtigungszertifikaten (IS-Zertifikate) für Inspektionssysteme autorisiert. Sowohl die Zugriffsrechte als auch die Gültigkeitsdauer der ausgestellten Zertifikate werden vom DV auf Basis der Anforderungen dieser CP definiert.

Von einem DV ausgestellte Zertifikate:

- IS-Zertifikate ( $C_{IS}$ )

Die folgende Tabelle enthält eine Übersicht der CVCA-ePass PKI mit deren Zertifizierungsstellen und der hiervon ausgestellten Zertifikate.

PKI-Instanz	Zertifizierungsstelle	Auszustellende Zertifikate
CVCA-ePass	CVCA-ePass-CA	$C_{CVCA}$ , Link- $C_{CVCA}$ , $C_{DV}$
DV	DVCA	$C_{IS}$
Inspektionssystem (IS)	keine	keine
Hoheitliches Dokument	keine	keine

Tabelle 3: Zertifizierungsstellen der CVCA-ePass PKI

### 1.3.2 Registrierungsstellen

Registrierungsstellen (Registration Authority, RA) führen vor der Ausstellung eines Zertifikats die zweifelsfreie Identifizierung und Authentifizierung des Antragstellers durch.

Die Registrierungsstelle der CVCA-ePass bildet die CVCA-ePass RA. Diese ist für die Bearbeitung der initialen Registrierungen sowie der möglichen Wiederholungsanträge von Document Verifiern zuständig.

Eine Registrierungsstelle der DV (Document Verifying Registration Authority, DVRA) ist hingegen für die Bearbeitung der initialen Registrierung sowie der möglichen Wiederholungsanträge von Inspektionssystemen zuständig.

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

PKI-Instanz	Registrierungsstellen	Eingehende Anträge
CVCA-ePass	CVCA-ePass-RA	Initialer C <sub>DV</sub> Zertifikatsantrag Wiederhol. C <sub>DV</sub> Zertifikatsantrag
DV national	DVRA	Initialer C <sub>IS</sub> Zertifikatsantrag Wiederhol. C <sub>IS</sub> Zertifikatsantrag
Inspektionssystem	keine	keine
Elektronische Ausweisdokumente	keine	keine

Tabelle 4: Registrierungsstellen (RAs) der CVCA-ePass PKI

### 1.3.3 Zertifikatsnehmer

Für die DV-Zertifikate gibt es drei Gruppen von Zertifikatsnehmern:

- deutsche Document Verifier, die auch die Berechtigung haben, Zertifikate bei anderen Nationen zu beantragen (DV national),
- deutsche Document Verifier, die nur bei der CVCA-ePass Zertifikate beantragen dürfen (DV national-begrenzt),
- ausländische Document Verifier, die über ihren SPOC bei der CVCA-ePass Zertifikate beantragen dürfen (DV international).

Zertifikatsnehmer sind CVCA-ePass, die Document Verifier und Inspektionssysteme.

Als Vertrauensanker stellt sich die CVCA-ePass ein selbst-signiertes Zertifikat aus.

Für die Ausstellung von Zertifikaten zum Zugriff auf die ePass-Anwendung für Inspektionssysteme benötigt ein Document Verifier die Berechtigung durch die CVCA-ePass. Hierfür stellt diese dem DV ein DV-Zertifikat aus.

Damit ein Inspektionssystem Zugriff auf die Daten eines hoheitlichen Dokuments erhalten kann, muss es hierzu über die Terminal Authentisierung [TR-03110] seine Berechtigung nachweisen. Diese Berechtigung wird in von einem DV ausgestellten IS-Zertifikat festgehalten und bestätigt.

### 1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind alle Einheiten, welche auf den Vertrauensanker der CVCA-ePass zurückgreifen, um Zertifikate der PKI zur Überprüfung von Berechtigungen zu verwenden.

Somit existieren die folgenden Zertifikatsnutzer in der CVCA-ePass PKI:

- CVCA-ePass, überprüft die Signatur der Wiederholungsanträge der DV,
- Document Verifier, überprüfen die Signatur der Wiederholungsanträge der Inspektionssysteme,
- hoheitliche Dokumente, überprüfen die Zertifikatskette zur Bestätigung der Zugriffsberechtigung eines Inspektionssystems.

### 1.3.5 Andere Teilnehmer

Teilnehmer, welche keine Verpflichtungen im Rahmen dieser Certificate Policy eingegangen sind, MÜSSEN zumindest die Bestimmungen der Zertifikatregeln der Europäischen Union aus [K(2008)8657] und [K(2009)7476] einhalten, um an die CVCA-ePass PKI angeschlossen werden zu können.

## 1.4 Verwendung von Zertifikaten

In diesem Abschnitt wird die erlaubte und verbotene Verwendung von Zertifikaten in der CVCA-ePass PKI definiert.

### 1.4.1 Erlaubte Verwendung von Zertifikaten

Schlüssel bzw. Zertifikate können von Zertifikatsnehmern zur Authentisierung sowie zur Erzeugung von elektronischen Signaturen verwendet werden.

Zertifikatsnutzer können Schlüssel bzw. Zertifikate zur Validierung von Authentisierungen und elektronischen Signaturen verwenden.

Daraus ergeben sich die folgenden Verwendungszwecke:

Zertifikat	Verwendungszweck und Eigenschaften
C <sub>CVCA</sub>	<ul style="list-style-type: none"> <li>Vertrauensanker der PKI. Daher wird der zugehörige öffentliche Schlüssel zur Überprüfung von Zertifikatsketten benötigt. Wird bei der Produktion im hoheitlichen Dokument gespeichert.</li> <li>Mit dem privaten Schlüssel werden das initiale C<sub>CVCA</sub>, die nachfolgenden Link-C<sub>CVCA</sub> sowie alle C<sub>DV</sub> und initiale Zertifikatsanträge von DV national an fremde CVCAAs signiert.</li> </ul>
Link-C <sub>CVCA</sub>	<ul style="list-style-type: none"> <li>Mit dem privaten Schlüssel des zuletzt gültigen C<sub>CVCA</sub> oder Link-C<sub>CVCA</sub> signiert.</li> <li>Aktualisiert den Vertrauensanker eines hoheitlichen Dokuments.</li> </ul>
C <sub>DV</sub>	<ul style="list-style-type: none"> <li>Der zugehörige öffentliche Schlüssel wird zur Überprüfung von Zertifikatsketten benötigt.</li> <li>Mit dem privaten Schlüssel werden Wiederholungsanträge signiert.</li> <li>Mit dem privaten Schlüssel werden C<sub>IS</sub> signiert.</li> </ul>
C <sub>IS</sub>	<ul style="list-style-type: none"> <li>Der zugehörige öffentliche Schlüssel wird zur Überprüfung von Zertifikatsketten benötigt.</li> <li>Mit dem privaten Schlüssel werden Wiederholungsanträge signiert.</li> <li>Mit dem privaten Schlüssel wird im Rahmen der Authentisierung gegenüber dem elektronischen Ausweisdokument eine Signatur erzeugt (siehe EAC-Protokollbeschreibung in [TR-03110]).</li> </ul>

Tabelle 5: Erlaubter Verwendungszweck von Zertifikaten und zugehöriger privater Schlüssel

**Hinweis:** Berechtigungszertifikate werden im nachfolgenden Text gemäß deren technischer Funktion als IS-Zertifikate (C<sub>IS</sub>) bezeichnet.

## 1.4.2 Verbotene Verwendung von Zertifikaten

Die Zertifikate dürfen ausschließlich gemäß ihres Verwendungszwecks (siehe Abschnitt 1.4.1) eingesetzt werden.

## 1.5 Administration der Policy

Die für dieses Dokument verantwortliche Organisation ist das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI kann über folgende Adresse kontaktiert werden:

<b>Organisation</b>	Bundesamt für Sicherheit in der Informationstechnik
<b>Einheit</b>	Referat 312 „Hoheitliche Dokumente und elektronische Ausweise“
<b>Adresse</b>	Godesberger Allee 185-189 53175 Bonn
<b>Fax</b>	+49 228 9582 55722
<b>E-Mail</b>	cvca-epass@bsi.bund.de
<b>Webseite</b>	<a href="https://www.bsi.bund.de/cvca-ePass">https://www.bsi.bund.de/cvca-ePass</a>

Tabelle 6: Kontaktdaten

### 1.5.1 Pflege der Certificate Policy

Jede aktualisierte Version der Certificate Policy wird den Anwendern unverzüglich über die Internetseite des BSI (siehe Abschnitt 1.5) zur Verfügung gestellt.

### 1.5.2 Zuständigkeit für das Dokument

Zuständig für Erweiterung und / oder nachträgliche Änderungen dieser CP ist das BSI.

### 1.5.3 Ansprechpartner / Kontaktperson

Siehe Abschnitt 1.5.

### 1.5.4 Zuständiger für die Anerkennung eines CPS

Das CPS ist ein internes Dokument. Dieses KANN aber bei Prüfungen herangezogen werden (siehe Abschnitt 8.1).

### 1.5.5 CPS-Aufnahmeverfahren

Das CPS MUSS die Anforderungen dieser CP umsetzen.

## 2 Veröffentlichungen und Aufbewahrung

### 2.1 Verzeichnisse

#### CVCA-ePass

Das BSI betreibt ein zentrales Verzeichnis, das **CVCA-ePass PKD**, als Bestandteil der CA. In diesem Verzeichnis werden alle produzierten Zertifikate gespeichert. Es beinhaltet:

- C<sub>CVCA</sub>/Link-C<sub>CVCA</sub>
- C<sub>DV</sub>

#### DV-Ebene

Die Document Verifier, DV national und DV national-begrenzt, MÜSSEN jeweils ein Verzeichnis mit Einträgen zu den von ihnen verwalteten Inspektionssystemen und den hierzu ausgestellten Zertifikaten einrichten. Diese Verzeichnisse werden im Sinne einer Bestandsführung und eines Archivs geführt und sind kontinuierlich zu pflegen (siehe [TR-03128], Kapitel 4.2.1.2 ff.).

Für DV international wird EMPFOHLEN, jeweils ein Verzeichnis mit Einträgen zu den von ihnen verwalteten Inspektionssystemen und den für diese ausgestellten Zertifikaten einzurichten und diese kontinuierlich zu pflegen.

Das Verzeichnis der CVCA-ePass, sowie die Verzeichnisse der DVs sind nicht öffentlich.

Die einzuhaltenden Aufbewahrungszeiten von Zertifikaten sind in Abschnitt 6.3.1 definiert.

### 2.2 Veröffentlichung von Informationen zur Zertifikatserstellung

#### 2.2.1 CVCA-ePass

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

- CVCA-ePass PKI Certificate Policy
- Verlinkung auf die mit dieser Policy in Verbindung stehenden technischen Richtlinien.
- Informationen zur Kommunikationsverbindung zum SPOC bzw. Kommunikationsschnittstelle gemäß [TR-03129].
- Zertifikate (siehe Abschnitt 4.5.1).

Das Certification Practice Statement (CPS) der CVCA-ePass wird nicht veröffentlicht.

#### 2.2.2 DV-Ebene

DV national und DV national-begrenzt MÜSSEN ihre **DV Certificate Policy** (siehe Abschnitt 5.1.2) veröffentlichen.

Für DV international wird EMPFOHLEN, seine **DV Certificate Policy** zu veröffentlichen.



## 2.3 Zeitpunkt und Häufigkeit der Veröffentlichungen

### CVCA-ePass

Die CVCA-ePass MUSS zu jeder Zeit alle weiteren Root-Zertifikate ( $C_{CVCA}$ , Link- $C_{CVCA}$ ), die für die Terminal-Authentisierung in der ePass-Anwendung (siehe [TR-03110]) erforderlich sind, bereitstellen.

Dies erfolgt über die Kommunikationsschnittstelle gemäß [TR-03129] bzw. [CSN369791] sowie über die BSI-Webseite.

Bei Änderungen an dieser CP MUSS die aktualisierte CP auf der BSI-CVCA-ePass Webseite veröffentlicht werden.

### DV-Ebene

Ein Document Verifier MUSS dem Inspektionssystem zu jeder Zeit alle weiteren für die ePass-Authentisierung (siehe [TR-03110]) erforderlichen Zertifikate und Rückruflisten ( $C_{CVCA}$ , Link- $C_{CVCA}$ ,  $C_{DV}$ , Masterliste und Defectliste) bereitstellen. Dies erfolgt für DV national und DV national-begrenzt über die Kommunikationsschnittstelle gemäß [TR-03129].

Wenn gemäß Abschnitt 2.2 eine Veröffentlichung der DV CP stattfindet, MUSS eine geänderte DV CP veröffentlicht werden und es MÜSSEN weiterhin die Anforderungen der CVCA-ePass CP übernommen werden.

Wird die Certificate Policy einer DV geändert, MUSS diese weiterhin die Anforderungen der CVCA-ePass CP entsprechen. Außerdem MUSS die geänderte Certificate Policy vor Inkrafttreten veröffentlicht werden.

## 2.4 Zugriffskontrollen auf Verzeichnisse

Die CVCA-ePass und die Document Verifier MÜSSEN durch geeignete organisatorische und technische Maßnahmen sicherstellen, dass die Vertraulichkeit und Integrität der Informationen in ihren Verzeichnissen gewahrt bleibt.

## 3 Identifizierung und Authentifizierung

Dieses Kapitel beschreibt die Prozeduren, die durchzuführen sind, um die Identität und Berechtigung eines Antragsstellers bei der **CVCA-ePass RA** oder **DVRA** vor dem Ausstellen eines Zertifikats festzustellen.

Das allgemeine Profil eines Zertifikatsantrags MUSS konform zu [TR-03110] sein.

### 3.1 Regeln für die Namensgebung

Der Bezeichner eines Schlüssels der CVCA-ePass PKI MUSS dem Profil in [TR-03110] entsprechen und wird im Feld `Certificate Holder Reference` angegeben.

#### 3.1.1 Arten von Namen

In diesem Abschnitt werden die Inhalte des Feldes `Certificate Holder Reference` (CHR) in den verschiedenen CV-Zertifikaten der CVCA-ePass PKI spezifiziert. Das Feld CHR bezeichnet den Eigentümer des Schlüssels.

##### CVCA-Zertifikat

Das Feld `Certificate Holder Reference` MUSS eines CVCA-Zertifikats aus den folgenden verketteten Elementen bestehen:

<i>Certificate Holder Reference</i>			
<i>Feld</i>	<b>Länderkürzel (Country Code)</b>	<b>Kürzel des Eigentümers (Holder Mnemonic)</b>	<b>Seriennummer (Sequence Number)</b>
<i>Inhalt</i>	DE	CVCAEPASS	<SN>
<i>Codierung</i>	ISO 3166-1 ALPHA-2	ISO/IEC 8859-1	ISO/IEC 8859-1 (00001 - 99999) <sup>1</sup>
<i>Länge</i>	2 Zeichen	9 Zeichen	5 Zeichen

##### DV-Zertifikat

Das Feld `Certificate Holder Reference` eines DV-Zertifikats MUSS aus den verketteten Elementen bestehen, welche im folgenden für jeden DV Typ erläutert werden.

##### DV national-begrenzt

Das Kürzel des Eigentümers KANN von dem beantragenden Document Verifier vor-geschlagen werden, die Festlegung des Kürzels MUSS aber durch die CVRA erfolgen.

<sup>1</sup> Bei Überlauf wird wieder bei 00001 begonnen

<i>Certificate Holder Reference</i>			
<i>Feld</i>	<b>Länderkürzel</b> Nation des DV <b>(Country Code)</b>	<b>Kürzel des Eigentümers</b> <b>(Holder Mnemonic)</b>	<b>Seriennummer</b> <b>(Sequence Number)</b>
<i>Inhalt</i>	DE	<Holder Mnemonic>	<SN>
<i>Codierung</i>	ISO 3166-1 ALPHA-2	ISO/IEC 8859-1	ISO/IEC 8859-1 (00001 - 99999) <sup>2</sup>
<i>Länge</i>	2 Zeichen	1-9 Zeichen	5 Zeichen

Tabelle 7: Certificate Holder Reference DV national-begrenzt

**DV national**

Das Kürzel des Eigentümers KANN von dem beantragenden Document Verifier vorgeschlagen werden, die Festlegung des Kürzels MUSS aber durch die CVRA erfolgen.

Da ein DV national Zertifikate bei ausländischen CVCAs beantragen kann, MUSS zusätzlich zum Länderkürzel der Nation des DV noch das Länderkürzel der Nation, bei der das Zertifikat beantragt wird, in der Certificate Holder Reference eingetragen werden.

<i>Certificate Holder Reference</i>				
<i>Feld</i>	<b>Länderkürzel</b> Nation des DV <b>(Country Code)</b>	<b>Kürzel des Eigentümers</b> <b>(Holder Mnemonic)</b>	<b>Länderkürzel</b> signierende Nation <b>(Country Code)</b>	<b>Seriennummer</b> <b>(Sequence Number)</b>
<i>Inhalt</i>	<CC>	<Holder Mnemonic>	<CC>	<SN>
<i>Codierung</i>	ISO 3166-1 ALPHA-2	ISO/IEC 8859-1	ISO 3166-1 ALPHA-2	ISO/IEC 8859-1 ( alpha-numerisch) <sup>3</sup>
<i>Länge</i>	2 Zeichen	1-9 Zeichen	2 Zeichen	3 Zeichen

Tabelle 8: Certificate Holder Reference DV national

2 Bei Überlauf wird wieder bei 00001 begonnen

3 Bei Überlauf wird wieder bei 001 begonnen

### **DV international**

Es wird EMPFOHLEN, dass die Document Verifier anderer Nationen die Certificate Holder Reference wie die DV national bilden. Die DV international MÜSSEN aber mindestens die Vorgaben des Anhangs der Kommissionsentscheidung der EU [K(2008)8657] (Anhang 1, Kapitel 3.1 Naming) einhalten.

### **Zertifikat des Inspektionssystems**

Das Feld Certificate Holder Reference eines IS-Zertifikats wird durch den für das Inspektionssystem zuständigen DV unter Berücksichtigung der [TR-03110] bestimmt.

### **3.1.2 Notwendigkeit für aussagefähige Namen**

Das Kürzel des Eigentümers in Zusammenhang mit dem Länderkürzel im Feld Certificate Holder Reference SOLLTE aus dem Namen des Eigentümers ableitbar sein.

### **3.1.3 Anonymität oder Pseudonymität von Zertifikatsnehmern**

Anonymität oder Pseudonymität von Zertifikatsnehmern ist nicht erlaubt.

### **3.1.4 Interpretationsregeln für verschiedene Namensformen**

Die Namen MÜSSEN durch die Certificate Holder Reference eindeutig definiert sein.

### **3.1.5 Eindeutigkeit von Namen**

Die Kombination von Länderkürzel und Kürzel des Eigentümers in der Certificate Holder Reference MUSS eindeutig einen bestimmten Zertifikatsnehmer identifizieren und DARF NICHT mehrfach vergeben werden.

### **3.1.6 Anerkennung, Authentifizierung und die Rolle von Markennamen**

Entfällt.

## 3.2 Initiale Überprüfung der Identität

In diesem Kapitel werden die Prozeduren zur Identifizierung und Authentifizierung des Zertifikatsnehmers für den initialen Zertifikatsantrag beschrieben.

Bestandteil dieser Prozeduren sind auch die Prüfungen nach den Anforderungen aus Abschnitt 8.1.

Auf der Wurzel-Ebene wird das Ausstellen des selbst-signierten CVCA-Zertifikats und von CVCA Link-Zertifikaten nicht betrachtet, da die CVCA-ePass RA und CVCA-ePass CA eine organisatorische Einheit, die CVCA-ePass, bilden. Somit ist eine Identifizierung und Authentifizierung auf Wurzel-Ebene gegeben.

### 3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Zum Nachweis des Besitzes des privaten Schlüssels MUSS der Zertifikatsantrag gemäß [TR-03110] eine sogenannte innere Signatur beinhalten. Hierzu wird der Zertifikatsantrag durch den Antragsteller mit dem zugehörigen privaten Schlüssel signiert.

Hierdurch MUSS bei der Antragsprüfung durch Verifikation der inneren Signatur mit dem im Zertifikatsantrag enthaltenden zugehörigen öffentlichen Schlüssel nachgewiesen werden, dass der Antragsteller im Besitz des privaten Schlüssels ist.

### 3.2.2 Authentifizierung von Organisationszugehörigkeiten

Die nachfolgenden Organisationen DÜRFEN innerhalb der CVCA-ePass PKI Zertifikatsanträge stellen. Hierbei wird speziell zwischen dem nationalen und dem ausländischen Bereich unterschieden. Die in diesem Abschnitt beschriebenen Anforderungen und Abläufe gelten für die **initiale** Identifizierung und Authentifizierung von Zertifikatsanträgen.

Die in dieser CP speziell in diesem Abschnitt angeführten Kommunikationszertifikate zur Absicherung der Kommunikationsverbindung zwischen den PKI-Instanzen MÜSSEN vergleichbar mit dem Sicherheitsniveau der V-PKI ([CP V-PKI]) sein.

#### **DV national und DV national-begrenzt**

Zur initialen Identifizierung und Authentifizierung eines Document Verifiers durch die CVCA-ePass Registrierungsstelle MUSS ein bevollmächtigter Vertreter des Betreibers persönlich erscheinen (dies gilt nicht für DV international).

Notwendige Unterlagen und Daten für die Registrierung sind:

- Antragsschreiben zur Zertifizierung durch die CVCA-ePass mit
  - Namen der Organisation (Behörde oder ein durch eine Behörde beauftragter privatwirtschaftlicher Dienstleister) und
  - Kontaktdaten der Ansprechpartner.
- Vertretungsvollmacht
- Bestätigung der hoheitlichen Verwendung des DV.
  - MUSS von der obersten Bundes- oder Landesbehörde ausgestellt werden und mit dem Dienstsiegel versehen sein.

- Certificate Policy des DV
  - MUSS die Anforderungen aus der CVCA-ePass CP berücksichtigen.
- Vereinbarung mit der CVCA-ePass, beinhaltet die
  - Erklärung der Einhaltung der Anforderungen der CVCA-ePass.
  - Bestätigung der erfolgreichen Testzertifizierung
    - Vor der initialen Identifizierung und Authentifizierung MUSS die Zertifikatsausstellung von der CVCA-ePass zum DV im Rahmen einer Testzertifizierung erfolgreich erprobt worden sein.
    - Die Testzertifizierung erfolgt auf Basis von Testschlüsseln unter Einhaltung der Anforderungen an den Wirkbetrieb aus [TR-03128] und dieser Certificate Policy.
    - Die verwendeten Testschlüssel (CVCA-ePass / DV) werden ausschließlich für den Testbetrieb erzeugt und DÜRFEN NICHT in den Wirkbetrieb zur Kommunikation mit hoheitlichen Dokumenten überführt werden.
- Kommunikationszertifikate (SSL-Client-Zertifikat und SSL-Server-Zertifikat, ggf. noch entsprechendes Wurzelzertifikat)
- Initialer Zertifikatsantrag (Initialer C<sub>DV</sub> Zertifikatsantrag, gemäß [TR-03110])
  - die Übergabe des Zertifikatsantrags MUSS durch den bevollmächtigten Vertreter erfolgen.

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

#### **DV international**

Ein ausländischer DV wird implizit durch die Registrierung seines nationalen SPOC registriert. Die Registrierung eines ausländischen SPOC wird in der Kommissionsentscheidung [K(2009)7476] definiert.

#### **Inspektionssysteme**

Der DV verantwortet den Einsatz der Inspektionssysteme in seinem Zuständigkeitsbereich, indem dieser berechtigten Inspektionssystemen IS-Zertifikate ausstellt. Somit MUSS der hoheitliche DV die Zertifikatsanträge der Inspektionssysteme prüfen. Des Weiteren MUSS dieser ein **Bestandsverzeichnis** aller von ihm verwalteten Inspektionssysteme und der zugehörigen Zertifikate führen.

Zur Identifizierung und Authentifizierung eines Inspektionssystems MUSS dessen Betreiber bei der hoheitlichen DVRA folgende Unterlagen und Daten einreichen:

- Antragsschreiben zur Zertifizierung durch den DV, beinhaltet:
  - Name der einsetzenden Behörde
  - Kontaktdaten der Ansprechpartner
- Technische Beschreibung des Inspektionssystems, beinhaltet:
  - Hersteller und Modellbezeichnung
  - Informationen zum Kryptografiemodul, inwiefern dieses hinsichtlich Sicherheitseigenschaften geprüft wurde, z.B. Common Criteria Zertifizierung.

- Eindeutige Kennung des Terminals
- Einsatzort
- Kommunikationszertifikat
- Initialer Zertifikatsantrag (Initialer C<sub>IS</sub> Zertifikatsantrag, gemäß [TR-03110])
  - Dieser wird vom Inspektionssystem direkt an den DV gesendet, nachdem der sichere SSL-Kanal durch Registrieren des Kommunikationszertifikats durch die hoheitlichen DVRA eingerichtet wurde. Die Kommunikation mit dem DV MUSS gemäß [TR-03129] erfolgen.

Die Registrierungsinformation aus den Unterlagen des Betreibers des Inspektionssystems MÜSSEN vom DV in dessen Bestandsverzeichnis vor dem Ausstellen eines Zertifikats für ein Inspektionssystem erfasst werden.

### **Sonderfall: EAC-Boxen**

EAC-Boxen sind Lesegeräte, die den Vorgaben aus [TR03131] entsprechen.

Bei der Produktion einer EAC-Box wird diese zur Signatur des initialen Zertifikatsantrags mit einem privaten Schlüssel versehen (SKey<sub>EAC-Box</sub>). Der zugehörige öffentliche Schlüssel (PKey<sub>EAC-Box</sub>) wird im Bestandsverzeichnis des zuständigen DV registriert. Zusätzlich wird ein Kommunikationszertifikat für eine sichere Kommunikation hinterlegt und dem Betreiber der EAC-Box ausgeliefert.

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

- Die SSL-Verbindung zum zuständigen DV MUSS mittels der hinterlegten Kommunikationszertifikate authentisiert werden.
- Der Zertifikatsantrag MUSS mit SKey<sub>EAC-Box</sub> signiert sein. Die Prüfung erfolgt mit PKey<sub>EAC-Box</sub> aus dem Verzeichnisdienst des zuständigen DV der unter dem entsprechenden Betreiber registriert sein MUSS.
- Der Wert des Felds Certificate Holder Reference MUSS dem vom zuständigen DV vorgegebenen Namensschema entsprechen.

### **3.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers**

Ein Zertifikatsantrag DARF NICHT von einer Einzelperson, sondern nur von einer Organisation gestellt werden.

### **3.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer**

Die Registrierungsstelle MUSS die Angaben zum Zertifikatsnehmer im Zertifikatsantrag gegen die eingereichten Unterlagen auf Korrektheit prüfen (siehe Abschnitt 3.2.2).

### **3.2.5 Prüfung der Berechtigung zur Antragstellung**

Siehe Abschnitt 3.2.

### 3.2.6 Kriterien für den Einsatz interoperierender Systeme/Einheiten

Entfällt.

## 3.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung

Nach der initialen Zertifikatsausstellung erfolgen sogenannte Wiederholungsanträge. Diese MÜSSEN ebenso wie die initialen Zertifikatsanträge (siehe Abschnitt 3.2) zweifelsfrei durch die Registrierungsstelle identifiziert und authentisiert werden.

Diese Certificate Policy unterscheidet zwei Arten von Wiederholungsanträgen:

- **Routinemäßige Wiederholungsanträge:** Der Antragssteller besitzt einen gültigen privaten Schlüssel dessen aktueller Einsatzzeitpunkt innerhalb des im zugehörigen Zertifikat definierten Gültigkeitszeitraums (d.h. zwischen den beiden Zeitpunkten definiert durch die Felder `Certificate Effective Date` und `Certificate Expiration Date`) liegt.
- **Nicht routinemäßige Wiederholungsanträge:** Der Antragssteller besitzt einen nicht mehr gültigen privaten Schlüssel dahingehend, dass dessen Einsatzzeitpunkt nicht innerhalb des im zugehörigen Zertifikat definierten Gültigkeitszeitraums (d.h. nicht zwischen den beiden Zeitpunkten definiert durch die Felder `Certificate Effective Date` und `Certificate Expiration Date`) liegt **oder** das sein Zertifikat von der übergeordneten Instanz für einen Wiederholungsantrag intern gesperrt wurde (interne Sperrliste).

Jede Certificate Authority der CVCA-ePass PKI MUSS einen Sperrdienst (interne Sperrliste) betreiben, um nicht routinemäßige Wiederholungsanträge erkennen zu können.

### 3.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung

Routinemäßige Wiederholungsanträge MÜSSEN folgende Eigenschaften zur Identifizierung und Authentifizierung durch die Registrierungsstelle erfüllen:

- Zustellung über
  - die in [TR-03129] definierten Kommunikationsprotokolle für DV national und DV national-begrenzt
  - die in [CSN369791] definierten Kommunikationsprotokolle für DV international
- Verbindungsauthentisierung über die bei der initialen Registrierung festgelegten Kommunikationszertifikate.
- Signatur des Zertifikatsantrags durch den Antragssteller mit einem noch gültigen, bei der CA registrierten Schlüsselpaar (gemäß Profil [TR-03110]).
- Der Bezeichner des Zertifikats (Wert des CHR-Feldes) MUSS den Vorgaben entsprechen (siehe Abschnitt 3.1).

Die genannten Anforderungen MÜSSEN durch die Registrierungsstelle geprüft werden. Hierzu verfügt diese über geeignete Mechanismen.



Inspektionssysteme stellen ihre routinemäßigen Wiederholungsanträge direkt an die Document Verifier, welche die entsprechenden Prüfungen durchführen.

### **3.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen**

Nach einem **nicht routinemäßigen Wiederholungsantrag** (siehe Einleitung 3.3) ist der Zertifikatsnehmer gesperrt. Der Bezug weiterer Zertifikate ist nicht möglich.

Um wieder Zertifikate erhalten zu können, MUSS der Zertifikatsnehmer die Gründe, warum kein routinemäßiger Wiederholungsantrag mehr durchgeführt wurde, melden (siehe Abschnitt 5.7). Danach MUSS der Zertifikatsnehmer einen neuen initialen Zertifikatsantrag übermitteln.

Die Identifizierung und Authentifizierung des neuen initialen Zertifikatsantrags wird in Abhängigkeit von der oben geforderten Begründung durchgeführt.

Wenn der nicht routinemäßige Wiederholungsantrag allein darin begründet war, dass nicht rechtzeitig ein routinemäßiger Wiederholungsantrag gestellt wurde, z.B. wegen technischer Schwierigkeiten, wird EMPFOHLEN den neuen initialen Zertifikatsantrag über die SSL-Verbindung zwischen den beiden PKI-Teilnehmern, mit dem bei der initialen Registrierung festgelegten Kommunikationszertifikat, zu versenden. Zusätzlich MUSS eine Prüfung des korrekten Fingerprints des neuen initialen Zertifikats-Requests durchgeführt werden. Die Übermittlung des Fingerprints MUSS über einen zur Internetverbindung unabhängigen Kommunikationskanal erfolgen, bspw. Telefon oder Fax.

In allen anderen Fällen MUSS die Übertragung des neuen initialen Zertifikatsantrags in Absprache mit der CVCA-ePass übermittelt und geprüft werden.

### **3.4 Identifizierung und Authentifizierung von Anträgen auf Sperrung**

Zertifikatsnehmer können sich selbst sperren, indem sie keinen routinemäßigen Wiederholungsantrag mehr stellen.

Sollte der Zertifikatsnehmer die Sperrung wieder aufheben wollen, MUSS der Grund für die Selbstsperrung gemeldet werden (siehe Abschnitt 5.7). Danach MUSS ein neuer initialer Zertifikatsantrag übersendet werden (siehe Abschnitt 3.3.2).

## 4 Betriebsanforderungen für den Lebenszyklus der Zertifikate

In diesem Kapitel werden die Prozeduren und Verantwortlichkeiten für den Lebenszyklus von Zertifikaten definiert. Dies umfasst insbesondere folgende Bereiche:

- Zertifikatsbeantragung
- Verarbeitung von Zertifikatsanträgen
- Zertifikatsausstellung

### 4.1 Zertifikatsantrag

Zertifikatsanträge für CVCA-Zertifikate werden von der CVCA-ePass selbst getätigt.

Von der DV-Ebene an abwärts gliedert sich die CVCA-ePass PKI in die Bereiche (siehe 1.1.2)

- national-begrenzt für nationale Zertifikatsnehmer, die nur bei der CVCA-ePass Zertifikate beantragen dürfen,
- national für nationale Zertifikatsnehmer, die bei der CVCA-ePass und fremden CVCA Zertifikate beantragen dürfen,
- international für Zertifikatsnehmer, die einer anderen Nation angehören, bei deren CVCA registriert sind und bei der CVCA-ePass Zertifikate beantragen dürfen.

Generell sind bei den Bereichen die folgenden Prozesse zu unterscheiden:

- Beantragung eines DV-Zertifikats ( $C_{DV}$ )
- Beantragung eines IS-Zertifikats ( $C_{IS}$ )

Hierbei ist hinsichtlich des Registrierungsdienstes zu berücksichtigen, ob es sich bei der Registrierung um einen initialen (Erstantrag) oder einen Wiederholungsantrag handelt.

#### 4.1.1 Wer kann einen Zertifikatsantrag stellen?

Zertifikatsanträge MÜSSEN über die in Kapitel 3 definierten Prozesse gestellt werden. In den in diesem Abschnitt aufgeführten Tabellen wird dargestellt, welche Organisationen Zertifikatsanträge stellen dürfen. Zur Antragstellung berechnigte nationale und national-begrenzte Document Verifier MÜSSEN alle Anforderungen gemäß [TR-03128] erfüllen.

Internationale Document Verifier MÜSSEN die Anforderungen der Zertifikatregeln aus [K(2009)7476] und [K(2008)8657] erfüllen.

Im Falle hoheitlicher Aufgabenstellungen erfolgt die Beantragung eines DV-Zertifikats ( $C_{DV}$ ) bei der CVCA-ePass immer durch den hoheitlichen Betreiber selbst, d.h. sowohl bei einem Erst- als auch bei einem Wiederholungsantrag.

Der Document Verifier ist selbst Antragsteller und Verantwortlicher für den Betrieb der ihm zugeordneten Inspektionssysteme. Deshalb werden die IS-Zertifikate ( $C_{IS}$ ) mittels eines Zertifikatsantrags des Inspektionssystems bei dem Document Verifier beantragt. Im Falle eines initialen Zertifikatsantrags wird das Inspektionssystem in die Bestandsführung des Document Verifiers

übernommen. Ausgenommen sind EAC-Boxen, diese sind schon vorher im Bestandsverzeichnis registriert (siehe Abschnitt 3.2.2).

Berechtigte Organisationen	Zertifikats-Typ	Zertifikatsantrag	
		Technische Annahme Zertifikatsantrag	Identifikation und Authentifizierung
DV	C <sub>DV</sub>	CVCA-ePass RA	CVCA-ePass RA
Betreiber des Inspektionssystems	C <sub>IS</sub>	DVRA	DVRA

Tabelle 9: Zur Zertifikatsantragsstellung berechtigte Organisationen

Zertifikatsanträge von DV national an fremde CVCA werden immer über den SPOC der CVCA-ePass gestellt. Erstanträge werden von der CVCA-ePass RA geprüft und durch die CVCA-ePass signiert, bevor sie an die entsprechende fremde CVCA weitergeleitet werden. Die Wiederholungsanträge werden nicht mehr von der CVCA-ePass RA geprüft, sondern lediglich an die entsprechende fremde CVCA weitergeleitet.

#### 4.1.2 Beantragungsprozess und Zuständigkeiten

Der Registrierungsprozess für ein Zertifikat wird durch den Zertifikatsantrag eines Antragsstellers initiiert. Der Zertifikatsantrag SOLL durch die jeweils zuständige RA auf Basis des 4-Augenprinzips geprüft werden. Sollten die Identifizierung und die Authentifizierung des Antragsstellers erfolgreich abgeschlossen worden sein, wird das entsprechende Zertifikat von der jeweiligen CA ausgestellt.

In diesem Abschnitt wird der Beantragungs- und Ausstellungsprozess sowie die Verantwortlichkeiten der verschiedenen CVCA-ePass PKI Instanzen definiert.

##### **Genereller Beantragungsprozess**

Der generelle Beantragungsprozess von Zertifikaten (C<sub>IS</sub>, C<sub>DV</sub>) bei der übergeordneten PKI-Instanz MUSS wie nachfolgend beschrieben erfolgen:

1. Der Antragsteller MUSS sein Schlüsselpaar unter Verwendung eines entsprechend sicheren Kryptografiemoduls generieren (siehe Abschnitt 6.2).
  - Auf DV- und Root-Ebene MÜSSEN die Schlüsselpaare in einer sicheren Umgebung erzeugt werden (siehe Abschnitt 5.1).
2. Der Antragsteller generiert den zugehörigen Zertifikatsantrag gemäß den Anforderungen aus Abschnitt 7.1.
3. Der Antragsteller sendet den Zertifikatsantrag an die entsprechende zuständige Stelle (siehe Tabellen in Abschnitt 4.1.1) über das entsprechende Kommunikationsprotokoll gemäß [TR-03129] bzw. [CSN369791] bei DV international.
4. Die zuständige RA führt eine Identifikation und Authentifizierung des Antragsstellers (beschrieben in Kapitel 3) durch. Die Vorgehensweise unterscheidet hier zwischen initialer Beantragung oder einem routinemäßigen Wiederholungsantrag.

5. Die zuständige CA erstellt nach der erfolgreichen Überprüfung des Antragsstellers und dessen Zertifikatsantrag (beschrieben in Kapitel 3) das entsprechende Zertifikat.

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

#### **Verantwortlichkeiten**

Nachfolgend werden die Hauptverantwortlichkeiten der RA und CA der jeweiligen PKI-Instanzen definiert. Hinzukommen die in Kapitel 8 definierten Prüfanforderungen.

#### **CVCA-ePass RA**

Die CVCA-ePass RA MUSS die folgenden Aufgaben wahrnehmen:

- Empfang von Zertifikatsanträgen für die CVCA-ePass über die in [TR-03129] und [CSN369791] definierten Schnittstellen.
  - Die Kommunikationsverbindung MUSS gegenseitig authentisiert und verschlüsselt sein.
- Überprüfung der Korrektheit des Zertifikatsantrags (gemäß Abschnitt 3.2) speziell unter folgenden Gesichtspunkten:
  - Ist der Antragssteller berechtigt, einen Zertifikatsantrag zu stellen?
  - Ist der Antrag konsistent?
  - Ist die vorgegebene Identität korrekt?
  - Besitzt der Antragssteller den zugehörigen privaten Schlüssel?
  - Ist der Antrag technisch konform (siehe Abschnitt 7.1)?
- Weiterleiten des technischen Zertifikatsantrags an die CVCA-ePass CA über eine gesicherte Verbindung.

#### **CVCA-ePass CA**

Die CVCA-ePass CA MUSS die folgenden Aufgaben wahrnehmen:

- Generierung von CVCA-ePass Schlüsselpaaren in einer sicheren Umgebung unter Verwendung eines sicheren Kryptografiemoduls (siehe Abschnitt 6.2).
- Ausstellen der CVCA-Zertifikate:  $C_{CVCA}$ , Link- $C_{CVCA}$  und Backup  $C_{CVCA}$ .
- Veröffentlichen der Zertifikate  $C_{CVCA}$ , Link- $C_{CVCA}$  und Backup  $C_{CVCA}$  auf der BSI-Webseite.
- Ausstellen von DV-Zertifikaten ( $C_{DV}$ ).
- Speicherung aller ausgestellten Zertifikate im CVCA-ePass PKD.

#### **DVRA**

Die DVRA MUSS die folgenden Aufgaben wahrnehmen:

- Empfang von Zertifikatsanträgen für die DVCA.
  - Die Kommunikationsverbindung MUSS gegenseitig authentisiert und verschlüsselt sein.

- Identifizieren und Authentifizieren des Terminal-Betreibers gemäß der in Kapitel 3.2 aufgeführten Prozeduren, speziell unter den folgenden Gesichtspunkten:
  - Ist der Antragssteller berechtigt, einen Zertifikatsantrag zu stellen?
  - Ist der Antrag technisch konform (siehe 7.1)?
  - Ist die vorgegebene Identität korrekt?
  - Besitzt der Antragssteller den zugehörigen privaten Schlüssel?
- Weiterleiten des technischen Zertifikatsantrags an die DVCA über eine gesicherte Verbindung.
- Führen eines Bestandsverzeichnisses in der alle, zur Zertifizierung berechtigten, Terminals und die hierfür ausgestellten Zertifikate registriert sind.

## DVCA

Die DVCA MUSS die folgenden Aufgaben wahrnehmen:

- Generieren von DV Schlüsselpaaren in einer sicheren Umgebung (siehe 5.1) unter Benutzung eines sicheren Kryptografiemoduls (siehe 6.2).
- Ausstellen von Inspektionssystem-Zertifikaten ( $C_{IS}$ ) für von der DVRA authentifizierte Betreiber des Inspektionssystems.
- Archivieren der ausgestellten Zertifikate (siehe Abschnitt 6.3.1).
- Zustellen des erzeugten Inspektionssystem-Zertifikats ( $C_{IS}$ ) mit der gesamten Zertifikatskette an das Inspektionssystem.

## Betreiber von Inspektionssystemen

Der Betreiber eines Inspektionssystems MUSS die folgenden Aufgaben wahrnehmen:

- Generieren von IS-Schlüsselpaaren mithilfe eines sicheren Kryptografiemoduls (siehe Anforderungen in Abschnitt 6.2).
- Durchführen der in Kapitel 3 aufgeführten Identifizierungs- und Authentifizierungsprozeduren.
- Prüfen von erhaltenen Zertifikaten auf Korrektheit.

## 4.2 Verarbeitung von Zertifikatsanträgen

In diesem Abschnitt werden die Prozeduren zur Verarbeitung von Zertifikatsanträgen beschrieben. Grundlage für die Verarbeitung ist die in Abschnitt 4.1 beschriebene Beantragung.

### 4.2.1 Durchführung der Identifizierung und Authentifizierung

Zertifikatsanträge MÜSSEN zur Prüfung der Gültigkeit des Zertifikatsantrags die entsprechenden Identifikations- und Authentifizierungsprozeduren durchlaufen. Hierbei werden zwei Fälle unterschieden:

- Initialer Zertifikatsantrag, Prozeduren beschrieben in Abschnitt 3.2

- Wiederholungsanträge, Prozeduren beschrieben in Abschnitt 3.3

Zertifikatsanträge dürfen ausschließlich an die nächsthöhere PKI-Instanz gestellt werden.

#### 4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Sollte eine Prüfung auf Basis der Identifikations- und Authentifizierungsprozeduren eines Zertifikatsantrags nicht erfolgreich verlaufen sein, so erhält der Antragssteller kein Zertifikat.

Im Falle eines nicht routinemäßigen Wiederholungsantrag ist gemäß Abschnitt 3.3 zu verfahren.

#### 4.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

In den Tabellen dieses Abschnitts sind die Fristen zur Reaktion auf einen Zertifikatsantrag aufgeführt. Hierbei wird insbesondere zwischen dem initialen Zertifikatsantrag und einem Wiederholungsantrag unterschieden.

Mit **Reaktionsfrist** ist hier der Zeitraum nach Eingang des Zertifikatsantrags bis zur Erstellung des Zertifikats, nach einer erfolgreichen Identifizierung und Authentifizierung, zu verstehen.

Beantragter Zertifikatstyp	Technische Annahme Request	Reaktionsfrist	
		Initialer Antrag	Wiederholungsantrag
C <sub>DV</sub>	CVCA-ePass RA	3 Werktage	3 Werktage

Tabelle 10: Fristen zur Bearbeitung von Zertifikatsanträgen

### 4.3 Ausgabe von Zertifikaten

In diesem Abschnitt werden die Prozeduren zur Ausgabe von Zertifikaten beschrieben. Grundlage für die Ausgabe ist die in Abschnitt 4.2 beschriebene Verarbeitung von Zertifikatsanträgen.

Die CVCA-ePass stellt für sich selbst CVCA-ePass Zertifikate (C<sub>CVCA</sub> und Link-C<sub>CVCA</sub>) aus.

Alle anderen PKI-Instanzen MÜSSEN Antragssteller erfolgreich als berechtigt identifizieren und authentifizieren (gemäß der in Kapitel 3 definierten Prozeduren), um diesem ein Zertifikat auszustellen zu können.

#### 4.3.1 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

Das ausgestellte Zertifikat wird dem Antragssteller über die in [TR-03129] bzw. bei DV international über die in [CSN369791] definierten Kommunikationsprotokolle zur Verfügung gestellt. Die Verbindung wird über die bei der initialen Registrierung hinterlegten Kommunikationszertifikate authentisiert und verschlüsselt.

## 4.4 Annahme von Zertifikaten

Nach Erhalt MUSS der Zertifikatsinhaber die Angaben im Zertifikat auf Korrektheit und Vollständigkeit prüfen. Um ein Zertifikat zurückzuweisen, MUSS der Inhaber eine Nachricht an die Zertifizierungsstelle schicken. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Bei fehlerhaften Zertifikaten sind, soweit möglich, die fehlerhaften bzw. unvollständigen Einträge zu benennen.

### Sonderfall EAC-Box

Im Falle einer Zurückweisung eines Zertifikats durch eine EAC-Box MUSS diese über die in [TR-03129] definierten Protokolle zur Fehlerübermittlung eine Nachricht an den DV senden. In einer solchen Nachricht ist der Grund für die Verweigerung der Annahme anzugeben. Zusätzlich sind soweit möglich die fehlerhaften bzw. unvollständigen Einträge im Zertifikat zu benennen. Die Absicherung der Integrität und Authentizität der Nachricht erfolgt durch die direkte SSL-Verbindung zwischen EAC-Box und DV.

### 4.4.1 Veröffentlichung von Zertifikaten durch die CA

Die CVCA-ePass MUSS deren CVCA-ePass Zertifikate ( $C_{CVCA}$ , Backup-  $C_{CVCA}$  und Link- $C_{CVCA}$ ) auf der BSI-CVCA- ePass Webseite veröffentlichen ([www.bsi.bund.de/cvca-ePass](http://www.bsi.bund.de/cvca-ePass)).

Überdies werden auf der BSI-Webseite ([www.bsi.bund.de/cvca](http://www.bsi.bund.de/cvca)) die CSCA-Zertifikate, CSCA Link-Zertifikate und die zugehörige Sperrliste zum Abruf bereitgestellt, welche zur Durchführung der passiven Authentisierung (siehe [TR-03110]) benötigt werden.

Die DV national und national-begrenzt MÜSSEN ihren Zertifikatsnehmern zusätzlich zu dem erstellten Zertifikat ( $C_{IS}$ ) die gesamte, für die ePass-Authentisierung erforderliche, Zertifikatskette (siehe [TR-03110]) über die Schnittstelle gemäß [TR-03129] zur Verfügung stellen.

## 4.5 Verwendung von Schlüsselpaar und Zertifikat

Die Zertifikate DÜRFEN NICHT für andere Verwendungszwecke als für die in Abschnitt 1.4 beschriebenen eingesetzt werden.

### 4.5.1 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Schlüssel bzw. Zertifikate können von Zertifikatsnehmern zum Nachweis einer Berechtigung sowie zur Erzeugung von elektronischen Signaturen verwendet werden. Nachfolgend werden für die verschiedenen PKI-Ebenen die erlaubten Verwendungen der privaten Schlüssel und der Zertifikate durch den Zertifikatsnehmer definiert:

#### Root-Ebene

Das Zertifikat der CVCA-ePass bildet den Vertrauensanker der CVCA-ePass PKI. Mit dem CVCA-Zertifikat ( $C_{CVCA}$ ) wird durch die CVCA-ePass die Berechtigung zur Ausstellung von DV-Zertifikaten nachgewiesen. Mit dem privaten Schlüssel werden das selbst signierte CVCA-ePass-Zertifikat ( $C_{CVCA}$ ), Backup-Zertifikate, die nachfolgenden Link-Zertifikate (Link- $C_{CVCA}$ ) sowie alle DV-Zertifikate ( $C_{DV}$ ) und Zertifikatsanträge von DV national an fremde CVCA signiert.

### **DV-Ebene**

Ein Document Verifier erbringt mit seinem DV-Zertifikat ( $C_{DV}$ ) den Nachweis der Berechtigung zur Ausstellung von IS-Zertifikaten. Mit dem privaten Schlüssel werden IS-Zertifikate ( $C_{IS}$ ) und Wiederholungsanträge an die CVCA-ePass signiert.

### **Inspektionssystems-Ebene**

Mit seinem Zertifikat ( $C_{IS}$ ) wird durch ein Inspektionssystem der Nachweis der Berechtigung erbracht, auf die Daten der ePass-Anwendung eines hoheitlichen Dokuments zugreifen zu dürfen. Dazu wird mit dem privaten Schlüssel im Rahmen der Authentisierung gegenüber dem hoheitlichen Dokument eine Signatur erzeugt (Protokollbeschreibung siehe [TR-03110] Terminal Authentication). Zudem werden mit dem privaten Schlüssel Wiederholungsanträge an den zuständigen DV signiert.

## **4.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer**

Zertifikatsnutzer können Schlüssel bzw. Zertifikate zur Validierung von Authentisierungen und elektronischen Signaturen verwenden.

Zertifikatsnutzer können die öffentlichen Schlüssel von Inspektionssystem, Document Verifiern und CVCA-ePass nutzen, um Zertifikatsketten und somit die Gültigkeit einer Berechtigung zu überprüfen.

## **4.6 Zertifikatserneuerung**

Zertifikatserneuerung bedeutet das Ausstellen eines neuen Zertifikats für einen öffentlichen Schlüssel, der bereits zertifiziert wurde.

Zertifikatserneuerung IST NICHT erlaubt.

## **4.7 Zertifizierung nach Schlüsselerneuerung**

Zertifizierung nach Schlüsselerneuerung bedeutet, dass ein Antragssteller (DV- oder Inspektionssystem-Ebene) ein neues Schlüsselpaar generiert und einen Zertifikatsantrag mit dem neuen öffentlichen Schlüssel einreicht. Dieser Zertifikatsantrag ist mit dem privaten Schlüssel signiert, welcher zum letzten Zertifikat gehört, welches von der CA ausgestellt wurde, bei der das neue Zertifikat beantragt wird.

Somit handelt es sich um einen Wiederholungsantrag.

### **4.7.1 Bedingungen der Zertifizierung nach Schlüsselerneuerungen**

Es muss sich um einen **routinemäßigen Wiederholungsantrag** gemäß Abschnitt 3.3 handeln.



#### **4.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?**

Die initiale Identifikation und Authentifizierung des Antragsstellers MUSS erfolgreich durchgeführt worden sein. Überdies muss der Antragssteller im Besitz eines noch gültigen privaten Schlüssels zur Signatur des neuen Zertifikatsantrags sein (siehe Abschnitt 3.3).

#### **4.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen**

Die Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen entspricht der Bearbeitung eines Wiederholungsantrags. Dieser Prozess ist in Abschnitt 3.3 beschrieben.

#### **4.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats**

Die Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats erfolgt, wie in Abschnitt 4.3.1 beschrieben.

#### **4.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen**

Das Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen wird in Abschnitt 4.4 beschrieben.

#### **4.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch die CA**

Die Veröffentlichung von Zertifikaten für Schlüsselerneuerungen entspricht den in Abschnitt 4.4.1 beschriebenen Regelungen.

#### **4.7.7 Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats**

Die Benachrichtigung anderer PKI-Teilnehmer über die Ausgabe eines Nachfolgezertifikats entspricht den Regelungen, beschrieben in Abschnitt 4.4.1.

### **4.8 Änderungen am Zertifikat**

Änderungen am Zertifikat bedeutet das Ausstellen eines neuen Zertifikats mit geänderten Zertifikatsinformationen aber gleich bleibendem öffentlichen Schlüssel.

Änderungen am Zertifikat DÜRFEN NICHT erfolgen.

### **4.9 Sperrung und Suspendierung von Zertifikaten**

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

Eine Sperrung erfolgt durch die Rücknahme einer erteilten Berechtigung. Eine Rücknahme löst aufgrund der kurzen Zertifikatslaufzeiten eine Sperrung in Form der Ablehnung weiterer

Zertifikatsanträge bzw. von Wiederholungsanträgen aus (siehe Prozeduren in den Abschnitten 3.3 und 3.4).

Jede PKI-Instanz, die Zertifikate ausstellt, MUSS Wiederholungsanträge sperren können z.B. über eine interne Sperrliste.

### **4.10 Service zur Statusabfrage von Zertifikaten**

In der CVCA-ePass PKI ist kein Service zur Statusabfrage von Zertifikaten vorgesehen.

Den Document Verifiern (DV national, DV national-begrenzt) MUSS es jederzeit möglich sein, den aktuellen Bestand der betreuten Inspektionssysteme mit den zugehörigen Zertifikaten sowie deren Historie festzustellen.

### **4.11 Beendigung der Teilnahme**

Die Beendigung der Teilnahme erfolgt durch das nicht mehr Stellen von routinemäßigen Wiederholungsanträgen (siehe Einleitung 3.3). Überdies MUSS die zuständige höhere PKI-Instanz entsprechend informiert werden.

Eine erneute initiale Überprüfung des Antragsstellers, wie in Abschnitt 3.2 definiert, ist erforderlich, um wieder an der CVCA-ePass PKI teilnehmen zu können.

### **4.12 Hinterlegung und Wiederherstellung von Schlüsseln**

Private Schlüssel DÜRFEN NICHT auf andere Art und Weise hinterlegt oder wiederhergestellt werden, als in Abschnitt 6.2 beschrieben.

## 5 Organisatorische, betriebliche und physikalische Sicherheitsmaßnahmen

### 5.1 Physikalische Sicherheitsmaßnahmen

In diesem Abschnitt werden die Anforderungen an die physikalischen Sicherheitsmaßnahmen der CVCA-ePass PKI Teilnehmer definiert.

#### 5.1.1 Generelle Sicherheitsmaßnahmen

Die nachfolgenden generellen Sicherheitsmaßnahmen MÜSSEN von

- der **CVCA-ePass** sowie
- den **Document Verifiern** (DV national, DV national-begrenzt)

der CVCA-ePass PKI sichergestellt werden. Für DV international gelten die entsprechenden Regeln aus [K(2008)8657] und [K(2009)7476].

Die Anforderungen beziehen sich insbesondere auf eine sichere Betriebsumgebung sowie die Betriebsabläufe von CA und RA:

- **Lage und Gebäude**  
Die CA und RA MÜSSEN beide in einem physikalisch geschützten Bereich betrieben werden.
- **Zugang**  
Die Zugänge zu CA und RA MÜSSEN kontrolliert und auditiert werden. Überdies wird der Zugang ausschließlich berechtigten Personen gewährt.
- **Stromversorgung**  
Eine unterbrechungsfreie Stromversorgung MUSS gewährleistet sein.
- **Wassergefährdung**  
Die IT-Infrastruktur der CA und RA MUSS gegen Wasserschäden aller Art geschützt werden.
- **Brandschutz**  
Gebräuchliche Methoden zum Schutz gegen Schäden durch Feuer MÜSSEN umgesetzt werden.
- **Speichermedien**  
Die Speichermedien MÜSSEN gegen nicht autorisierten oder unbeabsichtigten Gebrauch, hinsichtlich Zugang und Freigabe oder Schaden durch Personen oder andere Bedrohungen (z.B. Feuer oder Wasser) geschützt werden.
- **Abfallbeseitigung**  
Verfahren zur Beseitigung von Abfall MÜSSEN eingeführt werden, um unautorisierten Gebrauch, Zugang oder Freigabe von/zu vertraulichen Daten zu vermeiden.

- **Notfall-Backup**
  - Die Daten der CA und RA MÜSSEN gesichert werden (bspw. das Bestandsverzeichnis eines DV), sodass die Systeme nach einem Notfall/Unfall auf Basis dieser Daten wieder operativ betrieben werden können.
  - Backup- und Wiederherstellungsprozeduren DÜRFEN NICHT von anderen Personen als vertrauenswürdigen Betriebspersonal durchgeführt werden.
  - Ein Off-site Backup kritischer Daten SOLLTE durchgeführt werden. Dies betrifft insbesondere die Backup-Schlüssel und Zertifikate (siehe Abschnitt 5.6).

Es wird EMPFOHLEN, dass **Betreiber von Inspektionssystemen** je nach Einsatzumgebung ein entsprechendes Sicherheitsniveau angelehnt an die beschriebenen Anforderungen gewährleisten.

### 5.1.2 Erweiterte Sicherheitsmaßnahmen

Nationale und national-begrenzt Document Verifier unterliegen aufgrund deren Rolle gemäß [TR-03128] erweiterten Anforderungen bzgl. deren Sicherheitsmaßnahmen:

- **Nationale und national-begrenzte Document Verifier**  
MÜSSEN ein Sicherheitskonzept nach IT-Grundschutz erstellen. Darüber hinaus wird EMPFOHLEN, eine entsprechende Auditierung durchzuführen.

Darüber hinaus MÜSSEN alle Document Verifier (DV national und DV national-begrenzt) eine DV Certificate Policy erstellen, welche alle Anforderungen dieser Certificate Policy berücksichtigt. Darüber hinaus muss ein Certificate Practice Statement (CPS) erstellt werden. Eine Übersicht der erforderlichen Prüfungen, die ein solcher DV durchführen MUSS, ist in Abschnitt 8.1 enthalten.

## 5.2 Verfahrensanweisungen

Verfahrensanweisungen MÜSSEN umgesetzt werden, welche insbesondere die Trennung von Verantwortlichkeiten und die gegenseitige Kontrolle für kritische Vorgänge beinhalten. Die vertrauenswürdigen Rollen, die Anzahl an Personen, die für die Aufgabe benötigt werden und die Identifikation und Authentifizierung jeder Rolle sind in einem entsprechenden Konzept festzuhalten.

## 5.3 Personalkontrolle

Die PKI-relevanten Systeme der Teilnehmer an der CVCA-ePass PKI MÜSSEN von qualifiziertem und erfahrenem Personal betrieben werden.

Das Betriebspersonal der CVCA-ePass durchläuft eine Sicherheitsüberprüfung nach Sicherheitsüberprüfungsgesetz (SÜG).

## 5.4 Überwachungsmaßnahmen

Die Teilnehmer an der CVCA-ePass PKI MÜSSEN sicherstellen, dass deren Systeme über Protokollierungsmechanismen verfügen, um eine unberechtigte oder fehlerhafte Nutzung ihrer Systeme erkennen und analysieren zu können.

## 5.5 Archivierung von Aufzeichnungen

Die Teilnehmer an der CVCA-ePass PKI MÜSSEN sicherstellen, dass deren Systeme über angemessene Archivierungsfunktionen verfügen.

## 5.6 Schlüsselwechsel einer Zertifizierungsstelle

### CVCA-ePass (Root-Ebene)

Bei der Aufnahme des Wirkbetriebs generiert die CVCA-ePass das initiale **Root-Schlüsselpaar** und ein zugehöriges selbst-signiertes Zertifikat (Init  $C_{CVCA}$ ). Dieses selbst-signierte Zertifikat wird dem Ausweisproduzenten durch einen autorisierten Repräsentanten der CVCA-ePass übergeben und bei der Produktion in jedes hoheitliche Dokument als Vertrauensanker eingebracht.

Es MUSS ein **Backup für das Schlüsselmaterial der Root** erstellt werden, welches zumindest einer der folgenden Möglichkeiten entsprechen MUSS:

1. Es werden mindestens drei weitere **Backup-Schlüsselpaare** in entsprechend sicheren Hardwaremodulen generiert, welche die folgenden Anforderungen erfüllen MÜSSEN:
  - Alle Backup-Schlüsselpaare MÜSSEN Zertifikate erhalten, die mit dem aktiven privaten Root-Schlüssel signiert sind.
  - Alle Schlüsselpaare und zugehörige Zertifikate MÜSSEN sicher gelagert werden, entsprechend den diesbezüglichen Anforderungen dieser Policy.
  - Zwei Backup-Schlüsselpaare und die zugehörigen Zertifikate MÜSSEN in einer sicheren Umgebung gelagert werden, welche nicht zum Gebäude der CVCA-ePass gehört.
2. Es wird ein Schlüssel-Backup erstellt, welches den Anforderungen gemäß 6.2.3 entsprechen MUSS.

Vor Ablauf des aktiven Root-Schlüsselpaars (siehe Abschnitt 6.3.2) MUSS ein neues Root-Schlüsselpaar erzeugt werden. Das zugehörige **Link-Zertifikat** (Link- $C_{CVCA}$ ) MUSS folgende Anforderungen erfüllen:

- Das Link-Zertifikat MUSS vom noch aktiven privaten Root-Schlüssel signiert werden.
- Das erste selbst-signierte CVCA-Zertifikat und das aktuelle LINK-Zertifikat SOLLEN auf der BSI-Webseite veröffentlicht werden.

Alle für die Schlüsselgenerierung und -speicherung verwendeten Kryptografiemodule MÜSSEN die Anforderungen aus Abschnitt 6.2 erfüllen.

Die Gültigkeitszeiträume für die Zertifikate sind in Abschnitt 6.3.2 definiert.

### DV- / Inspektionssystem-Ebene

Teilnehmer auf DV- und Inspektionssystem-Ebene MÜSSEN für jeden Zertifikatsantrag ein neues Schlüsselpaar generieren (siehe Abschnitt 4.1.2) und die Anforderungen an einen routinemäßigen Wiederholungsantrag erfüllen (siehe Abschnitt 3.3).

## 5.7 Notfall-Management

In diesem Abschnitt werden Anforderungen an das Notfall-Management definiert. Insbesondere wird beschrieben, wie zu verfahren ist, wenn aufgrund eines Vorfalls kein routinemäßiger Wiederholungsantrag gestellt werden kann oder der Verdacht auf Kompromittierung bzw. Missbrauch des privaten Schlüssels besteht.

### 5.7.1 Behandlung von Vorfällen und Kompromittierung

Generell MÜSSEN alle Zertifikatsnehmer der CVCA-ePass PKI:

- **CVCA-ePass**
- **Bereiche national und national-begrenzt:** DV (siehe [TR-03128]) und Betreiber von Inspektionssystemen

ein Sicherheitskonzept erstellen, welches insbesondere die Kompromittierung des privaten Schlüssels berücksichtigt.

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

#### **Vorfall auf DV-Ebene**

##### **DV national und DV national-begrenzt:**

Kann aufgrund eines Vorfalls kein routinemäßiger Wiederholungsantrag gestellt werden oder besteht Verdacht auf Kompromittierung oder Missbrauch seines privaten Schlüssel, so MUSS der Document Verifier unverzüglich die CVCA-ePass informieren. Bei einem DV national MUSS die CVCA-ePass alle fremden CVCA informieren, von denen der entsprechende DV Zertifikate bezogen hat.

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

- Bericht über den Vorfall
- Protokolldaten
- In Relation stehende Betriebsdokumente

##### **DV international:**

Im Falle eines Vorfalls bei einem DV international sind die entsprechenden Vorgaben aus [K(2008)8657] und [K(2009)7476] einzuhalten.

#### **Vorfall auf Inspektionssystem-Ebene**

Kann aufgrund eines Vorfalls kein routinemäßiger Wiederholungsantrag gestellt werden oder besteht Verdacht auf Kompromittierung oder Missbrauch seines privaten Schlüssels, so MUSS der Betreiber des Inspektionssystems unverzüglich den zuständigen DV informieren. Der DV MUSS dies wiederum unverzüglich an die CVCA-ePass weitergeben. Handelt es sich um einen DV national muss die CVCA-ePass alle fremden CVCA informieren, von denen der entsprechende DV

Zertifikate bezogen hat. Zur Klärung des Vorfalls und der weiteren Vorgehensweise MUSS der Betreiber des Inspektionssystems dem DV folgende Unterlagen bereitstellen:

- Bericht über den Vorfall
- Protokolldaten
- In Relation stehende Betriebsdokumente

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

Wie die zuständige übergeordnete PKI-Instanz bei einem Vorfall zu verfahren hat, ist in Abschnitt 8.2 beschrieben.

### **5.7.2 Kompromittierung des privaten Schlüssels einer CA**

Bei Kompromittierung des privaten Schlüssels einer CA ist wie in Abschnitt 5.7.1 beschrieben zu verfahren.

## 6 Technische Sicherheitsmaßnahmen

### 6.1 Erzeugung und Installation von Schlüsselpaaren

Jeder Zertifikatsnehmer MUSS sein eigenes Schlüsselpaar generieren. Dies betrifft folgende Instanzen der CVCA-ePass PKI:

- CVCA-ePass (zertifiziert Schlüsselpaar selbst)
- DVs und Betreiber von Inspektionssystemen

#### 6.1.1 Erzeugung von Schlüsselpaaren

In der CVCA-ePass PKI dürfen ausschließlich kryptografische Algorithmen gemäß [TR-03110] eingesetzt werden. Die konkret zu verwendenden kryptografischen Algorithmen und Schlüssellängen für die Bereiche national und national-begrenzt sind in [TR-03116-2] angegeben.

Das jeweilige kryptografische Schlüsselpaar MUSS in einem sicheren Kryptografiemodul generiert werden (siehe Abschnitt 6.2).

Der technische Zugriff auf die Kryptografiemodule aller Zertifikatsnehmer ist durch ein Geheimnis geschützt (Passwort, PIN, o.ä.), welches nur die jeweiligen Operatoren kennen. Der Zugriff auf das Kryptografiemodul, insbesondere zur Schlüsselerzeugung, ist auf ein Minimum an Operatoren beschränkt.

Die Generierung von Schlüsseln durch die CVCA-ePass oder auf DV-Ebene erfordert die Einhaltung des 4-Augenprinzips. Zusätzlich MUSS die Generierung in einer sicheren Umgebung erfolgen.

#### 6.1.2 Lieferung privater Schlüssel an Zertifikatsnehmer

Der Zertifikatsnehmer generiert seinen privaten Schlüssel selbst. Daher wird keine Lieferung von privaten Schlüsseln vorgenommen.

#### 6.1.3 Lieferung öffentlicher Schlüssel an Zertifikatsherausgeber

Im allgemeinen MÜSSEN die Zertifikatsanträge der zuständigen Annahmestelle (siehe Abschnitt 4.1) über die in [TR-03129] (bzw. [CSN369791] für DV international) definierten Kommunikationsprotokolle zugestellt werden.

#### **Ausnahmen:**

Der **initiale Zertifikatsantrag MUSS** persönlich übergeben werden (siehe Abschnitt 3.2.2).

Sprechen **technische Gründe** gegen die Übertragung nach [TR-03129] (bzw. [CSN369791] für DV international), KANN die Übertragung auf einem anderen Weg stattfinden. Handelt es sich bei dem Zertifikatsantrag jedoch nicht um einen regulären Wiederholungsantrag, MUSS zusätzlich der Fingerprint des Zertifikatsantrags durch eine der Zertifizierungsstelle bekannte Person persönlich übergeben werden.



Der Fingerprint MUSS von der Zertifizierungsstelle geprüft werden.

#### **6.1.4 Lieferung öffentlicher Schlüssel der CA an Zertifikatsnutzer**

Die Zertifikate MÜSSEN dem Zertifikatsnutzer zugestellt werden. Dabei SOLLTEN die in [TR-03129] (bzw. [CSN369791] für DV international) definierten Kommunikationsprotokolle verwendet werden.

#### **6.1.5 Schlüssellängen und kryptografische Algorithmen**

Die zu verwendenden kryptografischen Algorithmen und Schlüssellängen sind in [TR-03116-2] und [TR-02102] definiert. Diese technische Richtlinie wird fortlaufend aktualisiert unter Berücksichtigung des aktuellen Technologie- und Wissensstands.

#### **6.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle**

Der Antragssteller MUSS sicherstellen, dass sein Zertifikatsantrag konform zu dem geforderten Profil in [TR-03110] und den Anforderungen dieser Policy ist.

Ferner MÜSSEN die Systeme des Antragsstellers eine automatische diesbezügliche Prüfung anschließend an die Generierung durchführen.

#### **6.1.7 Verwendungszweck der Schlüssel**

Die Schlüssel dürfen ausschließlich wie in Kapitel 4 beschrieben verwendet werden.

### **6.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module**

Der private Schlüssel MUSS in einem kryptografischen Hardwaremodul generiert, gespeichert und genutzt werden. Die **Kryptografiemodule** MÜSSEN nach den folgenden Common Criteria Protection Profiles (PPs) durch das BSI zertifiziert sein.

- High Security Module (HSM): PP-Cryptographic Modules "Enhanced" [PP-CM-e]
- Chipkarten: PP-Secure Signature-Creation Device [PP-SSCD].

Der Nachweis MUSS von einer durch das BSI für Common Criteria-Evaluierungen akkreditierte Prüfstelle erbracht werden.

In Ausnahmefällen kann von dieser Regelung abgewichen werden. Über die Zulässigkeit der Abweichung entscheidet das BSI.

#### **Zusätzliche Anforderungen für die EAC-Box:**

Eine EAC-Box MUSS konform zu [TR-03131] und nach [PP-IS] zertifiziert sein.

### **6.2.1 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln**

Das Prinzip der gegenseitigen Kontrolle MUSS bei der Zertifikatsausstellung durchgesetzt werden. Ein Operator für die Zertifikatsausstellung DARF KEIN Operator bei der RA sein.

### **6.2.2 Hinterlegung privater Schlüssel**

Es DARF KEINE Hinterlegung privater Schlüssel geben.

### **6.2.3 Backup privater Schlüssel**

Eine PKI-Instanz der CVCA-ePass PKI DARF NICHT über mehr als einen aktiven Schlüssel verfügen, der im Kryptografiemodul oder in einem Verbund (siehe Abschnitt 6.2.5) aus mehreren Kryptografiemodulen betrieben wird.

Dieser private Schlüssel KANN als Backup wie folgt exportiert werden:

- Verschlüsselter Dateicontainer
  - Datenstruktur, die den geheimen Schlüssel enthält und mit einem KEK (Key Encryption Key) verschlüsselt ist.
    - Die Anforderungen an die Verschlüsselung ergeben sich aus [TR-02102].
  - Die Nutzung des Dateicontainers erfordert den Import in ein Kryptografiemodul, das die Anforderungen aus Abschnitt 6.2 erfüllt.
  - Der Zugriff auf den verschlüsselten Dateicontainer MUSS auf das Betriebspersonal beschränkt sein.
- Backup Kryptografiemodul
  - Der private Schlüssel wird verschlüsselt direkt in das Backup-Kryptografiemodul transferiert (siehe Abschnitt 6.2.5).
  - Der Zugang zum Backup-Kryptografiemodul MUSS auf das Betriebspersonal beschränkt sein.

Der KEK (Key Encryption Key) der Kryptografiemodule zur Ver-/Entschlüsselung des privaten Schlüssels MUSS vertraulich ausgetauscht werden. Es MUSS sichergestellt sein, dass der KEK zu keinem Zeitpunkt vollständig im Klartext verfügbar ist.

Der private Schlüssel darf zu keinem Zeitpunkt außerhalb des Kryptografiemoduls im Klartext vorliegen.

Bei der Durchführung des Backups MUSS das Prinzip der gegenseitigen Kontrolle durchgesetzt werden.

### **6.2.4 Archivierung privater Schlüssel**

Es DARF KEINE Archivierung privater Schlüssel geben.

## 6.2.5 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Der private Schlüssel DARF zwischen kryptografischen Modulen transferiert werden. Hierdurch KANN ein Verbund aus Kryptografiemodulen gebildet werden bspw. zur Erhöhung der Ausfallsicherheit oder aus Lastverteilungsgründen.

Voraussetzung für den Transfer privater Schlüssel ist, dass nur Kryptografiemodule verwendet werden, welche die Anforderungen aus Abschnitt 6.2 erfüllen.

Der private Schlüssel MUSS hierbei verschlüsselt transferiert werden. Die Anforderungen an die Verschlüsselung ergeben sich aus [TR-02102]. Die Ver-/Entschlüsselung MUSS in den Kryptografiemodulen erfolgen.

Der KEK der Kryptografiemodule zur Ver-/Entschlüsselung des privaten Schlüssels MUSS vertraulich ausgetauscht werden. Es MUSS sichergestellt sein, dass der KEK zu keinem Zeitpunkt vollständig im Klartext verfügbar ist.

Bei der Durchführung des Transfers MUSS das Prinzip der gegenseitigen Kontrolle durchgesetzt werden.

## 6.2.6 Speicherung privater Schlüssel in kryptographischen Modulen

Das Kryptografiemodul MUSS die Anforderungen aus Abschnitt 6.2, welche eine sichere Speicherung des Schlüssels beinhaltet, berücksichtigen.

## 6.2.7 Aktivierung privater Schlüssel

Bei der Aktivierung wird der private Schlüssel in den Zustand versetzt, Signaturen erstellen zu können.

Die Aktivierung erfordert eine vorherige Authentisierung durch Eingabe eines Geheimnisses (Passwort oder PIN), EMPFOHLEN in Verbindung mit einem Hardware-Token.

Bei der Zertifikatsausstellung auf CVCA-Ebene MUSS das Prinzip der gegenseitigen Kontrolle durchgesetzt werden.

## 6.2.8 Deaktivierung privater Schlüssel

Bei der Deaktivierung MUSS der private Schlüssel in einen Zustand versetzt werden, in dem er ohne erneute Aktivierung keine Signaturen erstellen kann.

## 6.2.9 Zerstörung privater Schlüssel

Private Schlüssel auf Root- und DV-Ebene MÜSSEN zerstört werden, wenn deren Gültigkeitszeitraum abgelaufen ist.

Die Zerstörung erfolgt durch einen entsprechenden Mechanismus im HSM. Sollte der private Schlüssel auf einer Chipkarte gespeichert sein, MUSS diese physikalisch vernichtet werden.

## 6.2.10 Beurteilung kryptographischer Module

Die Anforderungen an Kryptografiemodule sind in Abschnitt 6.2 definiert.

## 6.3 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

### 6.3.1 Archivierung öffentlicher Schlüssel

Die PKI-Instanzen MÜSSEN verschiedene Zertifikate zur Durchführung deren Aufgabenstellung speichern. Die nachfolgende Tabelle zeigt eine Übersicht der Archivierungsdauer pro Ebene.

Ebene	Archivierungsort	Zertifikatstyp	Archivierungsdauer
CVCA-ePass	Internes CVCA-ePass PKD	$C_{CVCA}$ , LINK- $C_{CVCA}$	Zertifikatslaufzeit + 10,5 Jahre
		Alle ausgestellten $C_{DV}$	Zertifikatslaufzeit + 10,5 Jahre
		Alle signierten Zertifikatsanträge für DV national	10,5 Jahre
DV	Internes DV PKD	$C_{CVCA}$ und alle LINK- $C_{CVCA}$	Zertifikatslaufzeit + 2 Jahre
		Alle bezogenen $C_{DV}$	Zertifikatslaufzeit + 2 Jahre
		Alle ausgestellten $C_{IS}$	Zertifikatslaufzeit + 2 Jahre
Inspektionssystem	Zertifikatsspeicher	$C_{CVCA}$ und alle LINK- $C_{CVCA}$	Zertifikatslaufzeit + 6 Monate
		Aktuelle $C_{DV}$	Zertifikatslaufzeit + 6 Monate
		Aktuelle $C_{IS}$	Zertifikatslaufzeit + 6 Monate
Hoheitliches Dokument	Chipkarten-Speicher	$C_{CVCA}$ , LINK- $C_{CVCA}$	Gesamte Laufzeit (bzw. bis Ersetzung durch neues LINK- $C_{CVCA}$ )

Tabelle 11: Archivierung öffentlicher Schlüssel

Die Zertifikatslaufzeit entspricht dem Gültigkeitszeitraum des Zertifikats, beschrieben in Abschnitt 6.3.2.

### 6.3.2 Gültigkeitszeitraum von Zertifikaten und Schlüsselpaaren

In diesem Abschnitt wird der Gültigkeitszeitraum der Schlüssel der CVCA-ePass PKI definiert. Die Verwendungszwecke der Schlüssel und Zertifikate werden in Tabelle 6 angegeben.

Technisch wird der Gültigkeitszeitraum der Schlüssel durch die Zertifikatsgültigkeit bestimmt. Hierzu MUSS die jeweilige CA die entsprechenden Werte im auszustellenden CV-Zertifikat in den folgenden Feldern setzen:

Feld	Inhalt
Certificate Effective Date	Datum der Zertifikatsgenerierung
Certificate Expiration Date	Datum, an dem das Zertifikat abläuft.

Tabelle 12: Setzen von Gültigkeitszeiträumen in CV-Zertifikaten der CVCA-ePass PKI

Die nachfolgend aufgeführten Gültigkeitszeiträume für die Zertifikate der CVCA-ePass PKI MÜSSEN von der entsprechenden ausstellenden Instanz unter Einhaltung der Kodierungsanforderungen aus [TR-03110] gesetzt werden.

#### CVCA- und DV-Ebene

Die Gültigkeitszeiten auf CVCA- und DV-Ebene werden in der folgenden Tabelle dargestellt.

Ebene	Gültigkeitszeitraum
CVCA-ePass	6 Monate bis 3 Jahre
DV	2 Wochen bis 3 Monate

Tabelle 13: Gültigkeitszeiträume CVCA-ePass- und DV-Ebene

In der Regel werden die maximalen Gültigkeitszeiträume verwendet.

Die CVCA-ePass und die Document Verifier sollten darauf achten, rechtzeitig vor Ablauf ihrer Zertifikate ein neues Zertifikat zu beantragen, damit sie 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.

### Inspektionssystem-Ebene

Auf Inspektionssystem-Ebene sind die Gültigkeitszeiträume von Zertifikaten je nach Verwendungszweck und Betriebsart unterschiedlich. Die verschiedenen Inspektionssystem-Typen werden in Abschnitt 1.1 und [TR-03128] beschrieben.

Zertifikate auf Inspektionssystem-Ebene werden ausschließlich für die ePass-Authentisierung verwendet. Hier setzt sich der Gültigkeitszeitraum aus einer **Addition** von Zeiträumen zusammen, die wie folgt definiert sind:

- Nutzungszeit: Zeitraum, in dem das Zertifikat zur ePass-Authentisierung verwendet wird.
- Überlappungszeitraum: Zeitraum zur Beantragung eines neuen Zertifikats. Das Zertifikat kann innerhalb dieser Zeit noch zur Authentisierung verwendet werden.

Inspektionssystem	Anwendung	Betriebsart	Gültigkeitszeitraum	
			Nutzung	Überlappung
Inspektionssystem	Kontrollprozess	Verteilt	1 Monat	2 Tage
Inspektionssystem	Kontrollprozess	Integriert	1 Tag	1 Tag
Visualisierung	Auskunftsbegehren	Verteilt	1 Monat	2 Tage
Visualisierung EAC-Box	Auskunftsbegehren	Integriert	1 Tag	1 Tag
<b>Sonderfall</b>				
Inspektionssystem zur Qualitätskontrolle <sup>1</sup>	Produktionsprozess Qualitätssicherung	Integriert/ Verteilt	3 Monate	2 Wochen

Tabelle 14: Gültigkeitszeiträume in Inspektionssystemen

<sup>1</sup>Das Inspektionssystem zur Qualitätskontrolle DARF NICHT von anderen Institutionen als dem Ausweisproduzenten in dessen sicherer Produktionsumgebung betrieben werden.

## 6.4 Aktivierungsdaten

Siehe Abschnitt 6.2.7.

## 6.5 Sicherheitsmaßnahmen für die Rechneranlagen

Generell MÜSSEN alle an der CVCA-ePass PKI teilnehmenden Organisationen für ein angemessenes Sicherheitsniveau ihrer Rechneranlagen sorgen. Dies betrifft insbesondere:

- Implementierung und Pflege von Sicherheitskomponenten (Virens Scanner, Firewalls)
- Updatemanagement (regelmäßiges Installieren von Sicherheitsupdates)
- Umsetzung der Rollentrennung

- Implementierung und Betrieb von Protokollierungsmechanismen

Die Document Verifier MÜSSEN zusätzlich die in Abschnitt 5.1.2 definierten Anforderungen erfüllen.

## **6.6 Zeitstempel**

Entfällt.

## **6.7 Validierungsmodell**

Die Validierung der Zertifikate basiert auf dem Schalenmodell.

## 7 Profile für Zertifikate und Sperrlisten

### 7.1 Profile für Zertifikate und Zertifikatsanträge

Die in der CVCA-ePass PKI verwendeten Zertifikate sind selbst-beschreibende Card Verifiable Zertifikate (CV-Zertifikate) konform zum ISO Standard 7816 (ISO/IEC 7816-4:2005, ISO/IEC 7816-6:2004, ISO/IEC 7816-8:2004).

Das zu verwendende Profil für Zertifikate und Zertifikatsanträge ist in [TR-03110] spezifiziert. Unter anderem werden in dieser Richtlinie auch die Anforderungen an die Kodierung sowie die OIDs definiert.

Welche kryptografischen Verfahren und Schlüssellängen zu verwenden sind, ist in [TR-03116-2] festgelegt. Diese technische Richtlinie ist entscheidend für das Sicherheitsniveau der hoheitlichen Dokumente und wird daher fortlaufend aktualisiert.

Darüber hinaus enthält diese Policy Anforderungen für die Belegung folgender Zertifikats-Felder.

Feld	Bedeutung	Abschnitt
Certificate Holder Reference	Antragssteller	3.2
Certificate Effective Date Certificate Expiration Date	Gültigkeitszeitraum	6.3.2
Certificate Holder Authorization Template	Zugriffsrechte	7.1.1

Tabelle 15: Übersicht Felder CV-Zertifikat mit vorgegebener Wertebelegung

#### 7.1.1 Zugriffsrechte

Die CVCA-ePass MUSS die angegebenen Zugriffsrechte in den von ihr ausgestellten DV-Zertifikaten ( $C_{DV}$ ) im Feld Certificate Holder Authorization Template (CHAT) setzen. Diese Zugriffsrechte stellen das Maximum an Zugriffsrechten dar, die vom jeweiligen DV an ein Inspektionssystem über das IS-Zertifikat ( $C_{IS}$ ) weitergeben werden kann.

Document Verifier sind im Sinne der Datensparsamkeit angehalten, für IS-Zertifikate immer die minimal erforderlichen Zugriffsrechte zu gewähren.

Die folgende Tabelle 16 definiert, welche Zugriffsrechte über die Zertifikate der CVCA-ePass PKI gesetzt werden dürfen. Wie die Zugriffsrechte im CHAT zu kodieren sind, ist in Anhang C der [TR-03110] spezifiziert.



Erlaubte Zugriffsrechte für CVCA-/DV-Zertifikate <sup>4</sup>				
Auszustellender Zertifikatstyp	CVCA-ePass C <sub>CVCA</sub>	DV national C <sub>DV</sub>	DV national-begrenzt C <sub>DV</sub>	DV international C <sub>DV</sub>
DG 3 (Fingerabdrücke)	ja	ja	ja	ja

Tabelle 16: Erlaubte Zugriffsrechte für CVCA-/DV-Zertifikate

### 7.1.2 Zertifikatserweiterung

Die Zertifikate der CVCA-ePass PKI DÜRFEN KEINE Zertifikatserweiterungen enthalten.

## 7.2 Profile für Sperrlisten

In der CVCA-ePass PKI werden keine Sperrlisten ausgestellt.

Ausgenommen sind hiervon die internen Sperrlisten der RAs zum Sperren von Wiederholungsanträgen (siehe Abschnitt 3.3). Für diese wird kein Profil vorgegeben.

## 7.3 Profile für OCSP-Dienste

In der CVCA-ePass PKI werden keine OCSP-Dienste eingesetzt.

<sup>4</sup> Die Darstellung in der Tabelle entspricht nicht dem CHAT Aufbau (siehe [TR-03110]).

## 8 Überprüfung und andere Bewertungen

**Jeder Betreiber** einer PKI-Instanz der CVCA-ePass PKI verpflichtet sich zur Einhaltung dieser von der Wurzelinstanz (CVCA-ePass) herausgegebenen CP zur Durchführung eines ordnungsgemäßen Betriebs.

Die grundlegenden Prüfungsanforderungen an die verschiedenen PKI-Instanzen werden in Abschnitt 8.1 beschrieben.

Das Vorgehen bei identifizierten Mängeln ist in Abschnitt 8.2 definiert.

### 8.1 Inhalte, Häufigkeit und Methodik

In diesem Abschnitt werden die grundlegenden Prüfanforderungen für die PKI-Instanzen der CVCA-ePass PKI beschrieben.

#### CVCA-ePass (Root-Ebene)

Der Betrieb der CVCA-ePass MUSS in der sicheren Betriebsumgebung des BSI erfolgen. Diese erfüllt alle in dieser Certificate Policy definierten Anforderungen sowie die Sicherheitsanforderungen des IT-Grundschutzes.

#### DV-Ebene

Für die DV-Ebene ist ein „**Audit**“ ohne Zusatz wie z.B. „IT-Grundschutz“ wie folgt definiert:

- „Systematische unabhängige Untersuchung, inwieweit die realisierten, qualitätsbezogenen Tätigkeiten und die hieraus resultierenden Ergebnisse mit den geplanten Anforderungen übereinstimmen und geeignet sind, die Zielstellung zu erreichen.“
- Status des Auditors: 3rd Party = unabhängiger Auditor einer akkreditierten Zertifizierungsstelle (Akkreditierung nach DIN EN 45000 ff. und DIN EN/ISO 17000 ff.)
- Vorgehensweise: nach DIN ISO 19011 (Leitfaden für Audits von QMS/UMS)
- Informationssammlung mittels
  - Auswertung von Dokumenten
  - Befragung/Beobachtung von Tätigkeiten
  - Stichprobenartige Verifizierung insbesondere IT-gestützter Abläufe
- Untersuchungsgegenstand: Eingerichteter Betrieb der PKI-Instanz DV
- Prüftiefe: Wird im Einzelfall im Auditplan fixiert und ist system- und verfahrensorientiert.
- Systemorientierung = Struktur- und Funktionsaspekte (Aufbauorganisation, Dienste, Aufgaben, Personaleinsatz)
- Verfahrensorientierung = Prozessabläufe und Tätigkeiten (Ablauforganisation, Rollen)

Die nachfolgenden Tabellen enthalten die Prüfanforderungen für die PKI-Instanzen des nationalen und national-begrenzten Bereichs von der DV-Ebene bis zum Betreiber eines Inspektionssystems.

DV international MÜSSEN sich an die entsprechenden Vorgaben aus [K(2008)8657] halten.

Document Verifier				
Häufigkeit	Inhalt	Grundlage	Nachweis	Durchführung
<b>Initial</b> (Vor Aufnahme Wirkbetrieb)  Bei <b>Änderungen</b> am Pflichtenheft	Abnahme Pflichtenheft und DV CP <sup>1</sup> , IT- Sicherheitskonzept <sup>2</sup>	DV CP, CVCA-ePass CP, TRs, IT- Sicherheitskonzept, Pflichtenheft	Bestätigung	BSI
	Abnahme in Form eines Audits	CVCA- ePass CP, IT- Sicherheitskonzept, Pflichtenheft, CPS	Prüfbericht	DV beauftragt externe Prüfstelle
<b>Optional</b> (Empfohlen)	IT-Grundschutz Audit nach 27001	CVCA- ePass CP, TRs, IT- Sicherheitskonzept, Pflichtenheft, CPS	Zertifikat	DV beauftragt externen IT- Grundschutz Auditor

Tabelle 17: Prüfanforderungen Document Verifier

<sup>1</sup>Im Rahmen eines Auftragsverhältnisses für eine hoheitliche Stelle verpflichtend, sonst auf Wunsch (siehe [TR-03128]).

<sup>2</sup> Sichtung auf Eignung.

Betreiber von Inspektionssystemen				
Häufigkeit	Inhalt	Grundlage	Nachweis	Durchführung
<b>Initial</b> (Vor Aufnahme Wirkbetrieb)	Prüfung hoheitlicher Einsatz und sicheres Inspektionssystem (speziell Kryptomodul)	CVCA-ePass CP, TRs, Einsatz und Gerätebeschreibung	Berechtigung	zugehöriger DV

Tabelle 18: Prüfanforderungen Betreiber von Inspektionssystemen

## 8.2 Reaktionen auf identifizierte Vorfälle

### Initiale Prüfung

Die Teilnehmer der CVCA-ePass PKI MÜSSEN die entsprechenden in Abschnitt 8.1 aufgeführten Anforderungen an die initiale Prüfung ohne Mängel erfüllen, um mit dem Wirkbetrieb beginnen zu können.

Beim DV national MUSS die Prüfung alle 3 Jahre wiederholt werden.

### Vorfall im Betrieb

Ein Vorfall im Betrieb ist wie in Abschnitt 5.7.1 beschrieben, an die übergeordnete PKI-Instanz zu melden.

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.

Ist der Vorfall nicht sicherheitskritisch z.B. Defekt eines Kryptografiemoduls, so KANN ein erneuter initialer Zertifikatsantrag über die bestehende sichere SSL-Verbindung zugestellt werden (siehe Abschnitt 3.3.2).

## **9 Sonstige finanzielle und rechtliche Regelungen**

### **9.1 Preise**

Nachfolgend werden die preislichen Regelungen für die PKI-Instanzen der CVCA-ePass PKI angegeben.

#### **CVCA-ePass (Root-Ebene)**

Das Bundesamt für Sicherheit in der Informationstechnik, hier in seiner Funktion als Root der Public Key Infrastrukturen für hoheitliche Dokumente, erhebt gemäß § 1 BSI-KostV für Amtshandlungen nach § 3 Abs. 1 Nr. 3, 5, 6 und 7 des BSI-Errichtungsgesetzes Kosten nach der BSI-Kostenverordnung (BSI-KostV).

Zertifizierungen von Certification Authorities sind als solche Amtshandlungen anzusehen und mit einem festen Gebührensatz im Gebührenverzeichnis zur BSI-KostV verankert. Da Document Verifier ihrer Aufgabenstellung entsprechend CAs sind, besteht grundsätzlich eine Kostenerstattungspflicht für die Ausstellung von Berechtigungszertifikaten durch die Root.

#### **Ausnahmen**

Im Einzelfall wird geprüft, inwieweit sachlich oder persönlich begründete Gebührenfreiheit bzw. Ausnahmen nach dem Verwaltungskostengesetz (VwKostG) bestehen.

#### **DV-Ebene**

Eventuelle Gebühren für das Ausstellen von Zertifikaten oder Regi auf der DV-Ebene werden von der jeweiligen DV eigenständig geregelt.

### **9.2 Finanzielle Zuständigkeiten**

Die finanzielle Zuständigkeit des BSI obliegt den entsprechenden Regelungen der Bundesverwaltung.

Die Betreiber von PKI-Instanzen auf DV- und Terminal-Ebene sowohl hoheitlich als auch nicht hoheitlich sind finanziell für sich selbst zuständig.

## 10 Referenzen

- CP V-PKI: Bundesamt für Sicherheit in der Informationstechnik, Sicherheitsleitlinien der Wurzelzertifizierungsinstanz der Verwaltung
- CSN369791: Česká Technická Norma, ČSN 369791 – Information Technology – Country Verifying Certification Authority Key Management Protocol for SPOC
- PP-CM-e: Bundesamt für Sicherheit in der Informationstechnik, BSI-CC-PP-2009, Protection Profile - Cryptographic Modules, Security Level "Enhanced"
- PP-SSCD: CEN/ISSS, Protection Profile - Secure Signature-Creation Device, 2002
- PP-IS: Bundesamt für Sicherheit in der Informationstechnik, BSI-CC-PP-2010, Protection Profile for Inspection Systems (IS)
- K(2008)8657: Kommission der Europäischen Gemeinschaften, Entscheidung der Kommission vom 22.12.2008 über Zertifikatsregeln entsprechend der Vorgabe in den technischen Spezifikationen der Normen über Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten und zur Aktualisierung der Verweise auf Normen und Standards
- K(2009)7476: Kommission der Europäischen Gemeinschaften, Entscheidung der Kommission vom 5.10.2009 zur Änderung der Entscheidung der Kommission (K(2008) 8657 endgültig) über Zertifikatsregeln entsprechend der Vorgabe in den technischen Spezifikationen der Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten
- RFC 3647: Chokhani, S.; Ford, W.; Sabett, R.; Merrill, C.; Wu, S., Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, November 2003
- TR-02102: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-02102. Kryptografische Verfahren: Empfehlungen und Schlüssellängen
- TR-03110: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents
- TR-03116-2: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03116-2. eCard-Projekte der Bundesregierung
- TR-03128: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03128. EAC-PKI'n für den elektronischen Personalausweis
- TR-03129: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03129. PKI for the Extended Access Control (EAC), Protocol for the Management of Certificates and CRLs
- TR03131: Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03131 EAC-Box Architecture and Interfaces