Einführung der Gesundheitskarte

Spezifikation

CVC-Root

|  |  |
| --- | --- |
| Version: | 1.7.2 |
| Revision: | \main\rel\_online\rel\_ors1\rel\_opb1\24 |
| Stand: | 21.04.2017 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | [gemSpec\_CVC\_Root] |

Dokumentinformationen

**Änderungen zur Vorversion**

**Dokumentenhistorie**

| **Version** | **Stand** | **Kap./ Seite** | **Grund der Änderung, besondere Hinweise** | **Bearbeitung** |
| --- | --- | --- | --- | --- |
| 0.1.0 | 31.10.12 |  | Anlegen des Dokuments | Basis-TI Stufe 1 / PKI |
| 0.1.1 | 15.11.12 |  | Anpassung nach PKI-interner QS und Kommentierung durch PL und AM | Basis-TI Stufe 1 / PKI |
| 1.0.0 RC | 07.12.12 |  | Einarbeitung Gesellschafterkommentare | gematik |
| 1.1.0 | 06.06.13 |  | Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen) | gematik |
| 1.2.0 | 02.09.13 |  | Einarbeitung lt. Änderungsliste vom 08.08.2013 | gematik |
| 1.3.0 | 18.12.13 |  | Einarbeitung lt. Änderungsliste | gematik |
| 1.4.0 | 21.02.14 |  | Losübergreifende Synchronisation | gematik |
| 1.5.0 | 17.06.14 |  | Anpassung OID „rsaEncryption“ gemäß P11-Änderungsliste | gematik |
| 1.6.0 | 26.08.14 |  | Regelungen zum CVC-Root-Wechsel ergänzt | gematik |
| 1.7.0 | 24.08.16 |  | Anpassungen zum Online-Produktivbetrieb (Stufe 1) | gematik |
| 1.7.1 | 16.10.16 | A1 | Aufnahme SMC-B für Organisationen der Gesellschafter |  |
|  |  |  | P.14.9 | gematik |
| 1.7.2 | 21.04.17 |  | freigegeben | gematik |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 5](#_Toc486426730)

[1.1 Zielsetzung 5](#_Toc486426731)

[1.2 Zielgruppe 5](#_Toc486426732)

[1.3 Geltungsbereich 5](#_Toc486426733)

[1.4 Abgrenzungen 5](#_Toc486426734)

[1.5 Methodik 6](#_Toc486426735)

[2 Systemüberblick 7](#_Toc486426736)

[2.1 Hierarchie der PKI für CV-Zertifikate 7](#_Toc486426737)

[2.1.1 Zweck der CV-Zertifikate 7](#_Toc486426738)

[2.1.2 Überblick Infrastrukturen 7](#_Toc486426739)

[2.1.3 Hierarchie 8](#_Toc486426740)

[2.1.4 Vorgang und Vorteile 8](#_Toc486426741)

[3 Systemkontext 10](#_Toc486426742)

[3.1 Akteure und Rollen 10](#_Toc486426743)

[3.1.1 Anbieter der CVC-Root-CA 10](#_Toc486426744)

[3.1.2 TSP-CVC 10](#_Toc486426745)

[3.1.3 gematik 10](#_Toc486426746)

[3.1.4 Kartenherausgeber 10](#_Toc486426747)

[3.1.5 Kartenhersteller 11](#_Toc486426748)

[3.2 Nachbarsysteme 11](#_Toc486426749)

[3.3 Zugriffsprofile 12](#_Toc486426750)

[3.4 Sperren und Nachladen von CV-Zertifikaten der Kartengeneration 2 12](#_Toc486426751)

[4 Zerlegung des Produkttyps 13](#_Toc486426752)

[5 Übergreifende Festlegungen 14](#_Toc486426753)

[5.1 Erstellung Ausgabepolicy durch CVC-Root-CA 14](#_Toc486426754)

[5.2 Sicherheitskonzept CVC-Root-CA 14](#_Toc486426755)

[5.3 Zulassung 15](#_Toc486426756)

[5.4 Mindestanforderungen an eine CVC-Root-CA 15](#_Toc486426757)

[5.4.1 Schutzbedarfsfeststellung 15](#_Toc486426758)

[5.4.2 Verfügbarkeit der CVC-Root-CA 15](#_Toc486426759)

[5.4.3 Ausschließlichkeit und Dauer der Schlüsselnutzung 15](#_Toc486426760)

[5.4.4 Verlust der Zulassung 16](#_Toc486426761)

[5.4.5 Sicherheit des Schlüsselpaares 17](#_Toc486426762)

[5.4.6 Algorithmen und Schlüssellängen 20](#_Toc486426763)

[5.4.7 Schlüsselgenerationen und Schlüsselversionen 20](#_Toc486426764)

[5.4.8 Protokollierung 23](#_Toc486426765)

[5.4.9 Personelle Anforderungen 24](#_Toc486426766)

[5.4.10 Betriebliche Anforderungen 25](#_Toc486426767)

[5.5 Veröffentlichung von Informationen 26](#_Toc486426768)

[5.6 Verwaltung von Daten zur Zulassung und Registrierung 27](#_Toc486426769)

[5.7 Unterscheidung Produktiv-CVC-Root-CA und Test-CVC-Root-CA 28](#_Toc486426770)

[6 Funktionsmerkmale 29](#_Toc486426771)

[6.1 Ausstellung von CVC-CA-Zertifikaten durch die CVC-Root-CA 29](#_Toc486426772)

[6.1.1 Schnittstelle P\_Sub\_CA\_Certification\_CVC 29](#_Toc486426773)

[6.1.1.1 Schnittstellendefinition 29](#_Toc486426774)

[6.1.1.2 Umsetzung 30](#_Toc486426775)

[6.1.2 Artefakte 33](#_Toc486426776)

[6.1.2.1 CVC-PKCS#10-Request 33](#_Toc486426777)

[6.1.3 Testunterstützung 37](#_Toc486426778)

[6.2 Informationen zur Zulassung und Registrierung von TSP-CVC 37](#_Toc486426779)

[7 Anhang A – Verzeichnisse 39](#_Toc486426780)

[7.1 A1 – Abkürzungen 39](#_Toc486426781)

[7.2 A2 – Glossar 40](#_Toc486426782)

[7.3 A3 – Abbildungsverzeichnis 40](#_Toc486426783)

[7.4 A4 – Tabellenverzeichnis 40](#_Toc486426784)

[7.5 A5 - Referenzierte Dokumente 40](#_Toc486426785)

[7.5.1 A5.1 – Dokumente der gematik 40](#_Toc486426786)

[7.5.2 A5.2 – Weitere Dokumente 41](#_Toc486426787)

# Einordnung des Dokumentes

## Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen an den Produkttyp CVC-Root. Sie stellt Anforderungen hinsichtlich Konzeption und Betrieb der CVC-Root-CA im Umfeld der Kartengenerationen G1 und G2. Es werden übergreifende Festlegungen beschrieben sowie Anforderungen an die organisatorische Schnittstelle zum Erhalt eines CVC-CA-Zertifikates gestellt.

## Zielgruppe

Das Dokument richtet sich an Anbieter einer CVC-Root-CA und an Trust Service Provider CVC.

## Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

**Schutzrechts-/Patentrechtshinweis**

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifi­kation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Her­stellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifi­kation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter ver­stoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechts­inhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

## Abgrenzungen

Spezifiziert werden in diesem Dokument die von dem Produkttyp CVC-Root bereitgestellten (anderen Produkttypen oder Diensten angebotenen) Schnittstellen. Die von der CVC-Root benutzten Schnittstellen werden hingegen in den Spezifi­kationen derjenigen Produkttypen beschrieben, die diese Schnittstelle bereitstellen (siehe auch Anhang A5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps CVC-Root verzeichnet.

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zu folgenden Themenbereichen:

* Prozesse zur Zulassung und Registrierung eines TSP-CVC
* Festlegungen zur Ausgabe von X.509-Zertifikaten

Die Schnittstellen der TSP-CVCs (die CVC-Zertifikate für Endbenutzer ausgeben) werden in [gemSpec\_CVC\_TSP] beschrieben.

## Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuch­staben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

**⌦ TIP1-A\_nnnn <Titel der Afo>**

Text / Beschreibung

**⌫**

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

# 

# Systemüberblick

## Hierarchie der PKI für CV-Zertifikate

### Zweck der CV-Zertifikate

Die CV-Zertifikate werden zur C2C-Authentisierung von eGK, HBA und SMC verwendet. Bei Anwendung dienen die CV-Zertifikate für die vorgeschriebene gegenseitige Über­prüfung und Authentifizierung zwischen eGK und HBA (bzw. SMC).

### Überblick Infrastrukturen

Die aktuelle Public-Key-Infrastruktur (PKI) für die Karten der Generation 1 (G1) wird im Rah­men der fortschreitenden Entwicklungen (bessere Kryptoalgorithmen, bessere Chip­kar­ten, etc.) den stetig wachsenden Anforderungen (Internet, Portallösungen) nicht mehr gewachsen sein. Deshalb wird auch im CVC-Bereich die aktuelle G1-PKI in eine Infra­struktur G2 überführt werden.

Diese Migration erfolgt durch den Aufbau einer eigenständigen und unabhängigen PKI für G2. Zusätzlich zu der bereits vorhandenen G1-Root–CA und den dazu­ge­höri­gen CAs der zweiten Ebene wird dann eine G2-PKI hinzukommen. Die G2-Root ein­schließ­lich ihrer dazugehörigen Komponenten ist komplett autark. Es wird keinerlei Verbindungen (Cross-Zertifikate, Bridge-CAs) zwischen den Public-Key-Infrastrukturen G1 und G2 geben.

Für die Funktionalität der C2C-Authentisierung wird trotz des Wechsels der CVC-Root sowie der Umstellung der Kryptoalgorithmen von RSA auf ECC eine „weiche Migration“ auf die Kartengeneration G2 ermöglicht, indem HBA und SMC-B von Beginn an mit G1- wie auch mit G2-CV-Zertifikaten ausgestattet werden. Diese Karten können also mit eGKs der Generation G1 wie auch der Generation G2 interagieren.



G1

CV-PKI

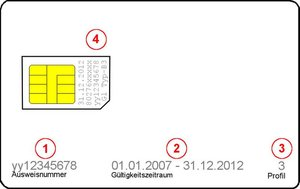
G2

CV-PKI

G2-eGK

HBA

G1-eGK



SMC-B

Abbildung 1: Karten mit CV-Zertifikaten unter verschiedenen CVC-Root-CAs

### Hierarchie

Die Struktur für das Ausbringen von CV-Zertifikaten ist in eine zweistufige Hierarchie ge­glie­dert (siehe Abbildung 2). Die CVC-Root-CA stellt den CVC-CAs (eGK, HBA, SMC) der zweiten Ebene die CVC-CA-Zertifikate aus. Die CVC-CAs (eGK, HBA, SMC) der zwei­ten Ebene wiederum stellen die CV-Zertifikate für die jeweiligen Chipkarten aus. Die­se Hierarchie und die Grundlagen der PKI für CV-Zertifikate sind in [gem­KPT\_PKI\_TIP#5] beschrieben. Vorgaben, inwiefern für unterschiedliche Kartenarten jeweils separate CVC-CAs nötig sind, werden nicht gemacht. Eine Separierung ergibt sich ab Kartengeneration 2 ggf. aus unterschiedlichen Laufzeiten der CV-CA-Zertifikate, siehe dazu Kap. 6.1.1.2.

CA-eGK

CA-HBA

Zertifikat eGK

Zertifikat HBA

Zertifikat SMC

CA-SMC



stellt Zertifikate aus für

Zertifikat eGK

Zertifi­kat eGK n+1



Zertifikat HBA

Zertifi­kat HBA n+1

Zertifikat SMC

Zertifi­kat SMC n+1

CVC-Root-CA

CA-eGK n+1

CA-HBA n+1

CA-SMC n+1

Abbildung 2: Beispielhafter Aufbau der CV-Hierarchie

### Vorgang und Vorteile

Die CVC-Root-CA stellt CV-Zertifikate für die CAs der zweiten Ebene aus. Die CV-Zer­tifi­ka­te für die Chipkarte (eGK, HBA, SMC) einschließlich der dazugehörigen karten­spe­zi­fischen Schlüssel werden von der CVC-CA eines Kartenherausgebers oder eines be­auf­trag­ten Dienstleisters ausgestellt.

Vorteile der zweistufigen PKI für die CV-Zertifikate sind,

* dass Kostenträger und Leistungserbringer für die CAs in ihrem Verant­wor­tungs­bereich (weitestgehend) eigene Vorgaben erstellen können,
* dass Kartenherausgeber für das Erzeugen der CV-Zertifikate für die von ihnen herausgegebenen Chipkarten (eGK, HBA, SMC) eigene CAs be­trei­ben können bzw. dafür geeignete Dienstleister beauftragen können,
* dass durch eine einzige übergeordnete CVC-Root-CA mittels Zertifi­zierung der zugehörigen CAs eine einheitliche PKI für die CV-Zertifikate entsteht.

# 

# Systemkontext

## Akteure und Rollen

### Anbieter der CVC-Root-CA

Der Anbieter der CVC-Root-CA betreibt als technischer Dienstleister im Auftrage der gematik die CVC-Root-CA. Hiermit generiert die CVC-Root-CA die CVC-CA-Zertifikate für die CVC-CAs der zweiten Ebene. Dabei stellt sie sicher, dass

* ein CVC-CA-Zertifikat nur für eine CVC-CA der zweiten Ebene generiert wird, falls der TSP-CVC aktuell gültig durch die gematik zugelassen sowie registriert ist und, sofern erforderlich, eine Qualifizierung für diese CVC-CA vorliegt und
* das Ausstellen eines CVC-CA-Zertifikats gemäß den Vorgaben aus Kapitel 6.1 geschieht.

Der Anbieter der CVC-Root-CA veröffentlicht den aktuellen öffentlichen Schlüssel der CVC-Root-CA.

### TSP-CVC

Ein TSP-CVC ist für das Generieren der CV-Zertifikate für eine Chipkarte (eGK, HBA, SM-B, gSMC) zuständig.

Ein TSP-CVC muss bei der gematik im Zuge eines organisatorischen Verfahrens zu­ge­lassen und die durch den TSP-CVC betriebenen CVC-CAs registriert werden.

Ein TSP-CVC muss das CVC-CA Zertifikat zur Generierung der CV-Zertifikate für eine Chip­karte vom Anbieter der CVC-Root-CA beziehen.

Die Anforderungen an einen TSP-CVC sind in der „Spezifikation – Trust Service Provider CVC“ [gemSpec\_CVC\_TSP] beschrieben.

### gematik

Die gematik fungiert als Zulassungsinstanz und Registrierungsstelle für TSP-CVC sowie für den Anbieter der CVC-Root-CA und legt die Sicherheitsanforderungen fest.

Die gematik stellt der CVC-Root-CA Informationen über zugelassene und registrierte TSP-CVC zur Verfügung, die berechtigt sind, CVC-CA-Zertifikate bei der CVC-Root-CA zu beziehen.

### Kartenherausgeber

Kartenherausgeber (Leistungserbringerorganisationen (LEOs), Kostenträger (KTR) und Gerätehersteller) sind für die Herausgabe von eGK, HBA, SMC-B, gSMC-K und gSMC-KT zuständig. Diese beauftragen jeweils einen TSP-CVC zur Produktion der gewünschten CV-Zer­ti­fi­ka­te. Es dürfen nur solche TSP-CVCs beauftragt werden, für die aktuell eine gültige Zulas­sung der gematik vorliegt. Für die eingesetzten CVC-CAs verfügt der TSP-CVC darüber hinaus über eine bei der gematik vorgenommene Registrierung sowie ggf. über eine Qualifizierung seitens der kartenherausgebenden Organisation.

### Kartenhersteller

Der Kartenhersteller ist bei der Produktion der Chipkarte für die sichere Einbringung der korrekten Schlüssel und Zertifikate in die Karte verantwortlich. Im Rahmen der Produktion einer Chipkarte (eGK, HBA, SM-B, gSMC) bringen die Kartenhersteller u.a. den aktuellen öffentlichen Schlüssel der CVC-Root-CA in die Chipkarte ein, der von der CVC-Root-CA bereitgestellt wird.

## Nachbarsysteme

Die Nachbarsysteme der CVC-Root-CA bestehen aus der gematik, den TSP-CVC sowie den Kartenherausgebern.

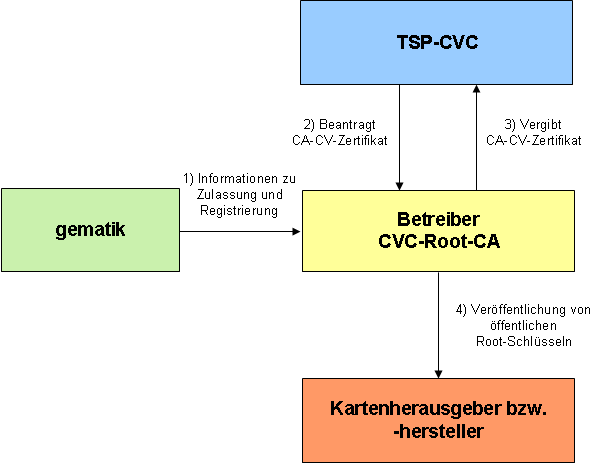


Abbildung 3: Nachbarsysteme der CVC-Root-CA

Für die Prozesse der Zulassung und Registrierung (Schritt 1) besteht eine organisa­torische Schnittstelle zur gematik (s. Abschnitt 6.2). Die gematik informiert den Anbieter der CVC-Root-CA regelmäßig über die aktuell zugelassenen TSP-CVC und registrierten CVC-CAs.

Für die Erzeugung der CVC-CA-Zertifikate des TSP-CVC bestehen technische und organi­sa­torische Schnittstellen (Schritte 2 und 3) zum Anbieter der CVC-Root-CA (s. Abschnitt 6.1).

Der öffentliche Schlüssel der CVC-Root-CA wird durch den Anbieter der CVC-Root-CA ver­öffentlicht (Schritt 4, vgl. Abschnitt 5.4.6). Kartenherausgeber bzw. Kartenhersteller benötigen den öffentlichen Root-Schlüssel für die Personalisierung der Karten.

## Zugriffsprofile

CVC-CA-Zertifikate für eine CVC-CA der Kartengeneration 1 enthalten kein Zugriffsprofil. Das Feld Card Holder Authorisation (CHA) wird in einem CVC-CA-Zertifikat nicht ange­ge­ben (vgl. [gemSpec\_PKI#6.5]).

CVC-CA-Zertifikate für eine CVC-CA der Kartengeneration 2 enthalten das Feld Card Holder Authorisation Template (CHAT), in dem die Rolle „CA unterhalb der Root-CA“ angegeben werden kann (vgl. [gemSpec\_PKI#6.7.5]).

## Sperren und Nachladen von CV-Zertifikaten der Karten­generation 2

Das Sperren und Nachladen von CV-Zertifikaten der Kartengeneration 2 wird aktuell nicht unterstützt.

# 

# Zerlegung des Produkttyps

Die CVC-Root-CA ist die zentrale Root-CA der PKI für alle CVC-CA-Zertifikate in der TI-Um­gebung. In [gemKPT\_Arch\_TIP#TIP1-A\_2245] wird die CVC-Root als Produkttyp defi­niert einschließlich der dazugehörigen Schnittstellen und Prozesse.

Der Prozess zur Generierung von CVC-CA-Zertifikaten durch die CVC-Root-CA verlangt vorab eine zwingende Regis­trierung der CVC-CA durch die gematik als oberste Registrierungsinstanz der TI. Danach können die weiteren Prozesse zur Erstellung durchgeführt werden. Siehe hierzu auch Kapitel 6.1.1.2.

Die Zertifikate für die eGK, den HBA und SMC werden durch die CVC-CA der zweiten Ebe­ne erzeugt.

Damit dieser Prozess erfolgreich von statten geht, benötigen die CVC-CAs der zweiten Ebe­ne ein eigenständiges CVC-CA-Zertifikat, dass durch die CVC-Root-CA ausgestellt wird.

# Übergreifende Festlegungen

## Erstellung Ausgabepolicy durch CVC-Root-CA

Gemäß [gemKPT\_PKI\_TIP#5.3] muss der Anbieter der CVC-Root-CA für die Produktion von CVC-CA-Zertifikaten eine Ausgabepolicy erstellen und deren Einhaltung durch geeignete Maßnahmen sicherstellen.

Die Ausgabepolicy enthält Anforderungen an die Sicherheit und den Betrieb einer CVC-Root-CA, die durch den Anbieter der CVC-Root-CA eingehalten werden. Die Darstellung, wie diese Anfor­derungen, insbesondere die Sicherheitsanforderungen, erfüllt werden, ist Gegenstand des Sicherheitskonzepts.

**⌦ TIP1-A\_5173 Inhalt der Ausgabepolicy der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS eine Ausgabepolicy erstellen, die mindestens die folgenden Punkte enthält: (a) An­gaben zum Betrieb der CA, (b) Angaben zu organisatorischen und technischen Sicher­heitsanforderungen, (c) Identifi­zierung von Antragstellern, die CVC-CA-Zertifi­ka­te beziehen möchten, (d) Fest­le­gungen von Namensregelungen zur CVC-Root-CA, (e) Angaben zu Zer­tifikats­profilen, (f) Wirtschaftliche und rechtliche Angelegenhei­ten sowie Anga­ben zur Haftung.

**⌫**

## Sicherheitskonzept CVC-Root-CA

Der Anbieter der CVC-Root-CA erstellt für den Betrieb der CVC-Root-CA ein Sicher­heitskonzept, das den Gesamtprozess von der Beantragung bis zur Ausgabe von CVC-CA-Zertifikaten an den Antragsteller beschreibt. Auf Verlangen der gematik GmbH weist der Anbieter der CVC-Root-CA die Einhaltung der im Sicherheitskonzept beschriebenen Maßnahmen nach.

Sind mehrere Organisationen an diesem Prozess beteiligt, sind die technischen- und orga­ni­satorischen Schnittstellen und Maßnahmen sowie deren Absicherung zu be­schrei­ben – ggf. auch durch Referenzierung der Sicherheitskonzepte der beteiligten Orga­ni­sa­tio­nen. Für Anforderungen an die Ausgestaltung und Vorgehensweise zum Sicher­heits­kon­zept siehe [gemSpec\_SiBetrUmg#AnhB].

**⌦ TIP1-A\_5174 Inhalt des Sicherheitskonzepts der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS ein Sicherheitskonzept gemäß den Vorgaben aus [gemSpec\_SiBetrUmg#AnhB] erstellen.

**⌫**

**⌦ TIP1-A\_5175 Darstellung der Zusammenarbeit verschiedener Organisationen**

In dem Sicherheitskonzept der CVC-Root-CA MUSS der Anbieter der CVC-Root-CA beschreiben, wie der Betrieb der CVC-Root-CA sowie Antrags- und Ausgabepro­zess organisiert sind und wie die entsprechenden Sicherheitsmaßnahmen bei den ein­zelnen Organisationen greifen.

**⌫**

## Zulassung

**⌦ TIP1-A\_5176 Betrieb der CVC-Root-CA nach Zulassung der gematik**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass er seinen Betrieb nur dann aufnimmt, wenn er über eine gültige Zulassung der gematik verfügt.

**⌫**

## Mindestanforderungen an eine CVC-Root-CA

In diesem Abschnitt werden die Mindestanforderungen an den Betrieb der CVC-Root-CA und die Ausgabe von CVC-CA-Zertifikaten definiert. Deren Einhaltung wird im Rahmen der Zulassung der CVC-Root-CA geprüft.

### Schutzbedarfsfeststellung

Der Anbieter der CVC-Root-CA für die Telematikinfrastruktur ist verpflichtet, die einheitlichen Methoden zu Datenschutz und Informationssicherheit anzuwenden, um Datenschutz- und Sicherheitskonzepte zu erstellen und zu pflegen oder die Anwendung äquivalen­ter Methoden ist von ihm nachzuweisen (vgl. [gemSpec\_Sich\_DS#GS-A\_2021].

### Verfügbarkeit der CVC-Root-CA

Anforderungen an die Verfügbarkeit der CVC-Root-CA werden nicht vorgegeben.

**⌦ TIP1-A\_5182 Verlust der Verfügbarkeit der CVC-Root-CA**

Bei einem dauerhaften Verlust der Verfügbarkeit des Produktiv- und/oder Testsys­tems der CVC-Root-CA MUSS der Anbieter der CVC-Root-CA die gematik sofort über den Verlust informieren.

**⌫**

### Ausschließlichkeit und Dauer der Schlüsselnutzung

**⌦ TIP1-A\_5183 Verwendung des Schlüsselpaars der CVC-Root-CA**

Der Anbieter einer CVC-Root-CA MUSS sicherstellen, dass das Schlüsselpaar einer CVC-Root-CA, ausschließlich für das Erstellen von Signaturen im Rahmen der Generierung von CVC-CA-Zertifikaten eingesetzt wird.

**⌫**

**⌦ TIP1-A\_5184 Begrenzung der Lebensdauer des Schlüsselpaars der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS das Schlüsselmanagement der CVC-Root-CA in seinem Sicherheitskonzept beschreiben und umsetzen.

**⌫**

Für jedes kryptographische Objekt (z.B. Schlüssel) müssen die relevanten Abläufe während des kompletten Lebenszyklusses festgelegt und dokumentiert werden.

**⌦ TIP1-A\_5185 Maximale Gültigkeitsdauer des Schlüsselpaars der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass die Lebensdauer des Schlüs­sel­paares der CVC-Root-CA eine Gültigkeitsdauer von zehn Jahren nicht überschreitet.

**⌫**

**⌦ TIP1-A\_5186 Ablauf der Gültigkeitsdauer des privaten Schlüssels der CVC-Root-CA**

Mit Ablauf der Gültigkeitsdauer DARF der private Schlüssel der CVC-Root-CA durch die CVC-Root-CA NICHT mehr für das Erstellen von Signaturen von CVC-CA-Zertifikaten der zweiten Ebene eingesetzt werden.

**⌫**

**⌦ TIP1-A\_5187 Weiterverwendung des privaten Schlüssels einer CVC-Root-CA**

Der Anbieter der CVC-Root-CA DARF den privaten Schlüssel der CVC-Root-CA NICHT mehr ver­wenden, nachdem die gematik die Zulassung des Anbieters der CVC-Root-CA widerrufen hat.

**⌫**

**⌦ TIP1-A\_5188 Vernichtung nicht mehr benötigter Schlüssel durch die CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass nicht mehr benötigte Schlüssel einer CVC-Root-CA sicher gelöscht werden.

**⌫**

### Verlust der Zulassung

**⌦ TIP1-A\_5189 Vernichtung der privaten Schlüssel bei Verlust der Zulassung der CVC-Root-CA**

Falls dem Anbieter der CVC-Root-CA die Zulassung der gematik entzogen wird, MUSS er alle privaten Schlüssel, die die CVC-Root-CA zur Erzeugung von CVC-CA-Zer­ti­fikaten besitzt, nach expliziter Anordnung der gematik vernichten.

**⌫**

**⌦ TIP1-A\_5190 Maßnahmen zur Vernichtung der Schlüsselpaare durch die CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass die Vernichtung von Schlüsseln durch eine der folgenden Maßnahmen realisiert wird: (a) physisches Löschen des privaten Schlüssels innerhalb des HSM, (b) dauerhaftes Sperren aller möglichen Zugriffe auf den privaten Schlüssel innerhalb des HSM.

**⌫**

**⌦ TIP1-A\_5191 Information über die Vernichtung aller Schlüsselpaare durch die CVC-Root-CA an gematik**

Der Anbieter der CVC-Root-CA MUSS der gematik die Vernichtung aller Schlüssel­paare schriftlich innerhalb von fünf Werktagen nach Eingang der Benachrichtigung über den Widerruf der Zulassung bestätigen.

**⌫**

### Sicherheit des Schlüsselpaares

**⌦ TIP1-A\_5192 Einsatz eines HSM, CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS für die Sicherheit des Schlüsselpaares einer CVC-Root-CA ein HSM einsetzen.

**⌫**

**⌦ TIP1-A\_5193 Schlüsselgenerierung im HSM der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS die Generierung eines neuen Schlüsselpaares in dem verwendeten HSM vornehmen.

**⌫**

**⌦ TIP1-A\_5194 Speicherung und Anwendung des privaten Schlüssels in einem HSM, CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass a) der private Schlüssel für die Er­zeu­gung von Zertifikaten nicht auslesbar in einem HSM gespeichert wird (einzige Ausnahme ist die Erstellung eines Schlüssel-Backups gemäß TIP1-A\_5204) und (b) nach Verwendung des privaten Schlüssels keine Artefakte der Bearbeitung im System hinterlassen werden, die eine Kompromittierung des Schlüssels ermöglichen oder erleichtern.

**⌫**

**⌦ TIP1-A\_5195 Einsatz einer Chipkarte als HSM, CVC-Root-CA**

Der Anbieter der CVC-Root-CA DARF NICHT eine Chipkarte als HSM einsetzen.

**⌫**

**⌦ TIP1-A\_5196 Ordnungsgemäße Sicherung des privaten Schlüssels der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS die ordnungsgemäße Sicherung des privaten Schlüssels der CVC-Root-CA nach dem aktuellen Stand der Technik gewährleisten und die An­forderungen an kryptographische Module im Rahmen seines betreiberspe­zifischen Sicherheitskonzeptes definieren.

**⌫**

**⌦ TIP1-A\_5197 Verwendung von privaten Schlüsseln einer CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS gewährleisten, dass a) alle kryptographischen Berech­nungen mit einem privaten Schlüssel der CVC-Root-CA intern in einem Hardware-Sicherheitsmodul (HSM) durchgeführt werden und b) private Schlüssel der CVC-Root-CA nicht im Klartext aus dem HSM exportiert werden können.

**⌫**

**⌦ TIP1-A\_5198 Evaluierung von HSMs – CVC-Root-CA**

Als HSM MUSS die CVC-Root-CA ein Modul einsetzen, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage. Die Prüftiefe MUSS mindestens (a) FIPS 140-2 Level 3, (b) Common Criteria EAL 4+ mit hohem Angriffspotenzial oder (c) ITSEC E3 der Stärke „hoch“ entsprechen.

**⌫**

Der private Schlüssel darf nicht mehr verwendet werden, wenn

* für seine Aufgaben ein neues Schlüsselpaar generiert und alle erforderlichen Maßnahmen zur Migration auf diese neuen Root-Schlüssel abgeschlossen sind.
* der Betrieb der CVC-Root-CA nach Entzug der Zulassung durch die gematik eingestellt wird.

**⌦ TIP1-A\_5199 Vorgaben an die Funktionalität des HSM der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS Hardware-Sicherheitsmodule (HSM) einsetzen, die min­destens Funktionen a) zur Generierung eines neuen Schlüsselpaares, b) zur Akti­vierung eines Schlüsselpaares, c) zum kryptographisch abgesicherten Import und Export eines privaten Schlüssels, d) zum (physikalischen) Löschen eines Schlüsselpaares, e) zur m-von-n-Aktivierung und f) zum Erstellen eines Zertifikats mit interaktiv einzugebenden Zertifikatsdaten beinhalten.

**⌫**

**⌦ TIP1-A\_5200 Nutzung eines HSM nach erfolgreicher Benutzerauthentisierung**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass das HSM nur nach einer erfolgreichen Benutzerauthentisierung genutzt werden kann.

**⌫**

Das genaue Vorgehen bei der Benutzerauthentisierung kann durch den Anbieter der CVC-Root-CA festgelegt werden. Sowohl eine Benutzerauthentisierung direkt gegenüber dem HSM als auch gegenüber der das HSM nutzenden Anwendung sind denkbar.

**⌦ TIP1-A\_5380 Zugang zu HSM-Systemen im Vier-Augen-Prinzip**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass alle Zugriffe auf das HSM und die direkt zur Administration des HSM verwendeten IT-Systeme im Vier-Augen-Prinzip erfolgen.

**⌫**

**⌦ TIP1-A\_5201 Speicherung und Auswahl von Schlüsselpaaren im HSM der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS ein Hardware-Sicherheitsmodul (HSM) einsetzen, das mehrere Schlüsselpaare speichern kann und über eine Funktion zur Aktivierung eines einzelnen spezifischen Schlüsselpaares verfügt, das nach erfolgter Auswahl zur Erzeugung von Zertifikaten verwendet wird.

**⌫**

**⌦ TIP1-A\_5202 Keine Weitergabe sensitiver Schlüssel durch die CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass eine Weitergabe geheimer und privater Schlüssel an andere Organisationen sowie an nicht berechtigte Personen nicht erfolgt.

**⌫**

**⌦ TIP1-A\_5203 Verwendung eines Backup-HSMs durch die CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS für das HSM der CVC-Root-CA ein Backup-HSM vorhalten.

**⌫**

**⌦ TIP1-A\_5204 Backup-HSMs – sicherer Schlüsseltransport CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS zur Übertragung von Schlüsselmaterial auf ein Backup-HSM sicherstellen, dass Vertraulichkeit und Integrität privater Schlüssel dabei zu jedem Zeitpunkt gewährleistet sind.

**⌫**

**⌦ TIP1-A\_5205 Schlüsselbackup bei der gematik**

Der Anbieter der CVC-Root-CA MUSS im Rahmen des mit dem BSI abgestimmten Konzepts "Verfahren zur Sicherung der CVC-Root-CA" die im Konzept definierten Mitwirkungspflichten erfüllen. Er muss im Rahmen des Konzeptes das für das Erzeugen von CVC-Sub-CA-Zertifikaten verwendete Schlüsselpaar für die Übergabe an die gematik exportieren.

**⌫**

**⌦ TIP1-A\_5206 Verfahrensbeschreibung Datensicherung der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS eine Verfahrensbeschreibung zur Datensicherung des CVC-Root-CA-Schlüsselpaars erstellen und mit der gematik abstimmen. Die Ver­fahrens­beschreibung beinhaltet mindestens die folgenden Punkte:

1. Beschreibung des zu sichernden Schlüsselmaterials
   1. Erzeugung
   2. Speicherung
   3. Lagerung
   4. (Wieder-) Einbringung
2. Organisatorische Maßnahmen
3. Beteiligte Rollen
4. Übergabe des Schlüsselmaterials zur Datensicherung bei der gematik

**⌫**

**⌦ TIP1-A\_5207 Quorum der Wiederherstellung**

Der Anbieter der CVC-Root-CA MUSS zur Wiederherstellung des Schlüsselmaterials einen Mecha­nismus zur Verfügung stellen, der die Anwendung der m-von-n-Aktivierung sicherstellt.

**⌫**

Durch die Anwendung der m-von-n-Aktivierung wird sichergestellt, dass eine Auslagerung des privaten Schlüssels in mehrere Schlüsselteile, z.B. auf Chipkarten, erfolgen kann. Zur Rekonstruktion des Schlüssels sind dann m von n Schlüsselteile (bzw. Chipkarten) erforderlich. Das Rollenkonzept zur Datensicherung des CVC-Root-CA-Schlüsselpaars muss beinhalten, dass jeder Geheimnisträger nur für die Verwahrung der ihm zuge­ordneten Schlüsselteile verantwortlich ist und mindestens *m* Geheimnisträger zusammen­kommen müssen, um den Schlüssel zu rekonstruieren.

**⌦ TIP1-A\_5208 Import aktuell genutzter CVC-Root-Schlüsselpaare**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass aktuell genutzte CVC-Root-Schlüssel­paare für Produktiv- und Test-PKI eines anderen Anbieters durch sein eigenes CVC-Root-CA-System unterstützt werden kann.

**⌫**

Das genaue Verfahren wird zwischen dem Anbieter der CVC-Root-CA und der gematik abgestimmt.

### Algorithmen und Schlüssellängen

Die durch die CVC-Root-CA zu verwendenden Algorithmen und Schlüssellängen werden durch [gemSpec\_Krypt#2.1.2] festgelegt. Aufgrund der durch die gematik vorgegebenen Schlüs­sellängen verfügen das Schlüsselpaar der CVC-Root-CA und die hiermit zertifi­zierten öffentlichen Schlüssel einer CVC-CA über die gleichen Schlüssellängen.

Vorgaben zur Migration von Algorithmen und Schlüssellängen und dabei zu beachtender Übergangsfristen sind in [gemSpec\_Krypt#3.14] definiert.

### Schlüsselgenerationen und Schlüsselversionen

Die CVC-Root-CA setzt für das Ausstellen von CVC-CA-Zertifikaten ein Schlüsselpaar ein, das eine vorgegebene Schlüssellänge hat. Ebenso wird das Schlüsselpaar nur mit einem bestimmten kryptographischen Algorithmus genutzt. Auf­grund fortschreitender Erkenntnisse bezüglich der Sicherheit bestimmter Schlüssellängen bzw. Algorithmen werden nach gewissen zeitlichen Abständen die Nutzung eines neuen (längeren) Schlüsselpaares und ggf. auch die Nutzung neuer kryptographischer Algo­rithmen für die CVC-Root-CA notwendig. Ein Wechsel zu einem neuen Schlüsselpaar mit einer größeren Schlüssellänge (und ggf. zu einem neuen Algorithmus) wird als Generationswechsel bezeichnet.

Es kann weitere Gründe für den Wechsel des Schlüsselpaares geben, wie z. B. organisa­torische Vorgaben (z. B. periodischer Wechsel des Schlüsselpaares) bzw. die Kompro­mit­tierung des aktuellen Schlüsselpaares. Hat das neue Schlüsselpaar die gleiche Länge, wie das alte Schlüsselpaar, wird ein solcher Wechsel des Schlüsselpaares durch die CVC-Root-CA als Versionswechsel bezeichnet. Bei einem Versionswechsel werden die genutzten krypto­graphischen Algorithmen nicht geändert.

Im Falle einer Kompromittierung eines Schlüsselpaares ist ein Versionswechsel als alleinige Maßnahme nicht ausreichend.

Kommt es bei der CVC-Root-CA zu einem Versionswechsel bei dem Schlüssel­paar für das Ausstellen von CVC-CA-Zertifikaten, kann dieser Fall logisch behandelt werden, wie das Aufsetzen einer neuen PKI für CV-Zertifikate. Eine übergeordnete CVC-Root-CA für alle Chipkarten existiert dann nicht mehr. Damit auch nach einem Wechsel der Root-Ver­sion die C2C-Authentisierung zwischen zwei Chipkarten noch durchgeführt werden kann, wird zwischen zwei Root-Versionen eine zweiseitige Cross-Zertifizierung vorgenommen (so­ge­nannte Cross-CV-Zertifikate vgl. [gemSpec\_PKI#Tab\_PKI\_937] werden dafür erzeugt). Da für CV-Zertifikate der Kartengeneration 1 kein Root-Wechsel mehr vorgesehen ist, erfolgt diese Vorgehensweise ausschließlich für CV-Zerti­fi­ka­te der Kartengeneration 2.

**⌦ TIP1-A\_5212 Wechsel der Schlüsselversion bei der CVC-Root-CA, Cross-Zertifizierung**

Im Falle eines Wechsels der Schlüsselversion MUSS die CVC-Root-CA ein Cross-CV-Zertifikat gemäß TAB\_PKI\_937 mit ihrem aktuellen privaten Schlüssel über ihren neuen öffentlichen Schlüssel erzeugen. Dabei ist das CED-Feld gleich der aktuellen Zeit und das CXD-Feld gleich dem Ende der Gültigkeit des der neuen Root-Version. Mit dem neuen Schlüsselpaar (neue Root-Version) MUSS die CVC-Root-CA ein Cross-CV-Zertifikat über den alten öffentlichen Schlüssel erzeugen, mit dem CED-Feld gleich der aktuellen Zeit und dem CXD dem Ende der 10-jähigen Laufzeit der alten Root (CXD aus dem selbstsignierten Root-Zertifikat der alten Root).

**⌫**

**⌦ TIP1-A\_5213 Wechsel der Schlüsselversion bei der CVC-Root-CA, Verfüg­bar­keit der Crosszertifizierungsdaten**

Im Falle eines Wechsels der Schlüsselversion MUSS die CVC-Root-CA die erzeugten Cross-CV-Zertifikate und selbstsignierten Root-Zertifikate auf einem Server der CVC-Root-CA Dritten zur Verfügung stellen.

**⌫**

**⌦ TIP1-A\_5214 Wechsel der Schlüsselversion bei der CVC-Root-CA**

Im Falle eines Wechsels der Schlüsselversion MUSS die CVC-Root-CA bei allen im Folgenden durch die CVC-Root-CA zu erzeugenden CVC-CA-Zertifikate ihr neues Schlüsselpaar verwenden.

**⌫**

**⌦ TIP1-A\_5215 Planmäßiger Wechsel der Schlüsselversion bei der CVC-Root-CA**

Im Falle eines planmäßigen Wechsels der Schlüsselversion MUSS die CVC-Root-CA den Wechsel zwei Jahre nach dem letzten Wechsel vornehmen.

**⌫**

**⌦ TIP1-A\_5216 Planmäßiger Wechsel der Schlüsselversion bei der CVC-Root-CA, Erzeugung des Cross-Zertifikats**

Im Falle eines planmäßigen Wechsels der Schlüsselversion MUSS die CVC-Root-CA spätestens zwei Wochen nach dem Wechsel Cross-CV-Zertifikate und das selbstsignierte Root-Zertifikat veröffentlichen (vgl. TIP1-A\_5213).

**⌫**

**⌦ TIP1-A\_5217 Planmäßiger Wechsel der Schlüsselversion bei der CVC-Root-CA, Entscheidung über den Versionswechsel**

Die gematik MUSS die Entscheidung über die Durchführung eines planmäßigen Wechsels der Schlüsselversion spätestens vier Monate vor dem geplanten Termin treffen.

**⌫**

**⌦ TIP1-A\_5218 Unplanmäßiger Wechsel der Schlüsselversion bei der CVC-Root-CA**

Im Falle eines ungeplanten Wechsels der Schlüsselversion der CVC-Root-CA durch  
(a) Betreiberwechsel gleich aus welchem Grund,   
(b) Änderungen im Kryptokatalog, oder Notfallszenario gemäß [gemRL\_Betr\_TI#10] KANN der Anbieter der CVC-Root-CA den Wechsel außerhalb des geplanten Turnus vornehmen.

**⌫**

Ein Versionswechsel bei dem Schlüsselpaar bei der CVC-Root-CA wird auch als Wechsel der Root-Version bezeichnet. Alle CV-Zertifikate, die direkt (CV-Zertifikate für eine CVC-CA) bzw. indirekt (CV-Zertifikate für eine eGK/HBA/SM-B/gSMC) von einem bestimmten Schlüsselpaar der Root-CA abhängen, gehören zur gleichen Root-Version.

Unabhängig davon, ob eine neue Schlüsselgeneration oder Schlüsselversion erstellt wird, muss jede Generierung eines CVC-Root-CA-Schlüssels durch die gematik angeordnet werden.

**⌦ TIP1-A\_5219 Schlüsselerzeugung nach Anordnung durch die gematik**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass eine Schlüsselgenerierung aus­schließ­lich nach Anordnung durch die gematik erfolgen kann. Der Anbieter der CVC-Root-CA MUSS überprüfen, ob der Auftrag der gematik mindestens die folgenden An­gaben enthält: (a) Datum des Auftrags, (b) Namen von zwei verantwortlichen Mitar­beitern der gematik, (c) Indikator, ob es sich um einen „planmäßigen“ oder einen „notfall­mäßigen“ Schlüsselwechsel bzw. um eine initiale Schlüsselgenerierung han­delt, (d) Vorgabe für die Länge des neuen Schlüsselpaares und des zu verwen­denden Algorithmus, (e) Unterschriften von zwei verantwortlichen Mitarbeitern der gematik.

**⌫**

### Protokollierung

**⌦ TIP1-A\_5220 Protokollierung durch die CVC-Root-CA - Ereignisse**

Der Anbieter der CVC-Root-CA MUSS seine Aktivitäten revisionssicher protokollieren. Mindestens die folgenden Ereignisse MÜSSEN durch die CVC-Root-CA protokolliert werden: (a) Generierung eines neuen Schlüsselpaares im HSM, (b) Aktivierung eines Schlüssel­paares, (c) Löschung eines privaten Schlüssels im HSM, (d) Export des privaten Schlüssels, (e) Import des privaten Schlüssels, (f) Sperrung der Zugriffe auf einen privaten Schlüssel im HSM, (g) Erzeugen eines CVC-CA-Zertifikats (h) Zugriffe auf den privaten CVC-Root-CA-Schlüssel.

**⌫**

**⌦ TIP1-A\_5221 Protokollierung durch die CVC-Root-CA – Werte pro Ereignis**

Bei der Protokollierung MÜSSEN durch die CVC-Root-CA die folgenden Werte pro­to­kolliert werden: (a) Datum und Uhrzeit, (b) Typ des Ereignisses, (c) Namen der beteiligten Mitarbeiter der CVC-Root-CA, die das HSM freigeschaltet haben.

**⌫**

**⌦ TIP1-A\_5222 Protokollierung durch die CVC-Root-CA – Generierung eines neuen Schlüsselpaares**

Bei dem Erzeugen eines neuen Schlüsselpaares MÜSSEN durch die CVC-Root-CA zu­sätzlich die folgenden Werte protokolliert werden: (a) Datum des Auftrags der gematik, (b) Namen der beiden verantwortlichen Mitarbeiter der gematik (aus dem Auftrag) (c) Fingerprint des öffentlichen Root-Schlüssels des neu generierten Schlüsselpaars.

**⌫**

**⌦ TIP1-A\_5223 Protokollierung durch die CVC-Root-CA – Aktivierung eines neuen Schlüsselpaares**

Bei der Aktivierung eines Schlüsselpaares MÜSSEN durch die CVC-Root-CA zu­sätzlich die folgenden Werte protokolliert werden: (a) Datum des Auftrags der gematik, (b) Namen der beiden verantwortlichen Mitarbeiter der gematik (aus dem Auftrag) (c) Fingerprint des öffentlichen Root-Schlüssels des aktivierten Schlüssel­paars.

**⌫**

**⌦ TIP1-A\_5224 Protokollierung durch die CVC-Root-CA – Erzeugung eines CVC-CA-Zertifikats**

Bei dem initialen Erzeugen eines CVC-CA-Zertifikates MÜSSEN durch die CVC-Root-CA zu­sätzlich die folgenden Werte protokolliert werden: (a) Name und Anschrift des be­an­tragenden TSP-CVC, (b) Datum des Antrags (aus dem schriftlichen Antrag), (c) Na­me der CVC-CA für die das CVC-CA-Zertifikat erstellt wird, (d) Fingerprint über den öffentlichen Schlüssel der CVC-CA, für die das neue CVC-CA-Zertifikat erstellt wer­den soll, (e) Name und Geburtsdatum des Mitarbeiters des TSP-CVC, (f) sig­nierter CVC-PKCS#10-Request, (g) Inhalt der Felder CHR bei Kartengeneration 1 und Inhalt der Felder CHR und CHAT bei Kartengeneration 2, (h) das erstellte CVC-CA-Zertifikat selber.

**⌫**

**⌦ TIP1-A\_5225 Nachvollziehbarkeit bei Produktion von CVC-CA-Zertifikaten**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass nachträglich anhand der Protokolle nachvollzogen werden kann, wann wie viele CVC-CA-Zertifikate für welchen TSP-CVC erzeugt wurden.

**⌫**

**⌦ TIP1-A\_5226 Schutz der Protokolldaten gegen Manipulation**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass alle Protokolldaten bei ihrer Erstellung, Verarbeitung und Speicherung geeignet gegen mögliche Manipulationen geschützt werden. Dies beinhaltet auch den Schutz vor Verlust von Protokolldaten.

**⌫**

**⌦ TIP1-A\_5227 Prüfung der Protokolldaten durch die gematik**

Auf Antrag MUSS die CVC-Root-CA Vertretern der gematik Einblick in die Proto­kolle gewähren. Der Anbieter der CVC-Root-CA MUSS dazu sicherstellen, dass die Protokoll­daten in menschenlesbarer Form vorliegen.

**⌫**

### Personelle Anforderungen

**⌦ TIP1-A\_5228 Berücksichtigung von Rollen**

Der Anbieter der CVC-Root-CA MUSS in seinem organisatorischen Teil des Sicher­heits­konzepts mindestens die folgenden Rollen unterscheiden: (a) Leiter CVC-Root-CA, (b) Sicherheitsbeauftragter CVC-Root-CA, (c) Zertifizierer, (d) Datenschutz­be­auftragter, (e) Geheimnisträger.

**⌫**

Mit "Leiter CVC-Root-CA" wird der Leiter der CVC-Root-CA bezeichnet. Der "Sicher­heits­beauf­tragte CVC-Root-CA" ist eine vom "Leiter CVC-Root-CA" ernannte Person, die die Aufgabe Infor­mationssicherheit koordiniert und vorantreibt. Die Rolle "Zertifizierer" ist dabei für das Generieren von CVC-CA-Zertifikaten für zugelassene TSP-CVCs zuständig. Der Datenschutzbeauftragte ist eine vom "Leiter CVC-Root-CA" bestellte Person, die für den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personen­be­zogenen Daten verantwortlich ist. Die Rolle "Geheimnisträger" ist verantwortlich für die Organisation zur Verwahrung von Schlüsselteilen.

**⌦ TIP1-A\_5229 Definition der Rollen in der CVC-Root-CA und Festlegungen ihrer Aufgaben**

Der Anbieter der CVC-Root-CA MUSS in seinem Sicherheitskonzept die genauen Auf­ga­ben der Rollen beschreiben. Geklärt werden MUSS dabei, welche verschie­den­en Rollen nicht durch eine einzelne Person ausgeübt werden dürfen (Rollenaus­schluss­matrix). Dargestellt werden MUSS insbesondere, welche Funktionen des HSM durch eine Rolle genutzt werden können.

**⌫**

**⌦ TIP1-A\_5230 Benennung von Mitarbeitern gegenüber der gematik durch die CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS der gematik die verantwortlichen Mitarbeiter für die Rollen "Leiter CVC-Root-CA", "Sicherheitsbeauftragter CVC-Root-CA" und „Zertifizierer“ mitteilen. Für die Rolle "Leiter CVC-Root-CA" MUSS dabei auch ein Stellvertreter genannt werden. Der Anbieter der CVC-Root-CA MUSS der gematik Änderungen an der Zuordnung von Rollen mitteilen.

**⌫**

**⌦ TIP1-A\_5231 Berücksichtigung von Zugriffen auf das HSM im Vier-Augen-Prinzip, CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass keine einzelne Person zwei Rol­len ausüben kann, die Zugriffe auf das HSM im Vier-Augen-Prinzip für diese ein­zelne Person ermöglichen.

**⌫**

### Betriebliche Anforderungen

**⌦ TIP1-A\_5232 Umsetzung der definierten Prozesse durch die CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS die definierten Prozesse umsetzen.

**⌫**

**⌦ TIP1-A\_5233 Geschützter Bereich der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS das HSM in einem geschützten Bereich der Betriebsstätte unterbringen. Für diesen Bereich der Betriebsstätte der CVC-Root-CA MUSS gelten: (a) Der Zugang zu diesem Bereich ist nur autorisierten Mitarbeitern möglich. (b) Beim Zugang muss der Mitarbeiter eindeutig identifiziert werden. (c) Der Zugang zu diesem Bereich wird protokolliert. (d) Alle Zugänge sind in ge­eig­ne­ter Weise gegen Einbruch gesichert. (e) Ist kein berechtigter Mitarbeiter an­we­send, wird der Bereich alarmüberwacht. (f) Besuchern ist der Zugang nur in Be­gleitung au­to­risierter Mitarbeiter und nur zu notwendigen, im Sicherheitskonzept be­schrieben­en Zwecken erlaubt.

**⌫**

**⌦ TIP1-A\_5234 Verwendung mehrerer geschützter Bereiche der CVC-Root-CA**

Eine CVC-Root-CA KANN verteilt in mehreren geschützten Bereichen betrieben werden.

**⌫**

**⌦ TIP1-A\_5235 Schutz von HSM der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS Maßnahmen beschreiben, ergreifen und nach­weisen, die verhindern, dass ein HSM bzw. ein Backup-HSM aus einem der geschützten Bereiche unautorisiert entfernt werden kann.

**⌫**

**⌦ TIP1-A\_5236 Zugriffe auf Systeme der CVC-Root-CA über Arbeitsplatzrechner (oder Systeme) außerhalb des geschützten Bereichs**

Falls zur CVC-Root-CA gehörende Arbeitsplatzrechner (oder Systeme) außerhalb des geschützten Bereichs Zugriffe auf Systeme der CVC-Root-CA in dem ge­schütz­ten Bereich haben, MUSS der Anbieter der CVC-Root-CA sicherstellen, dass alle Zu­griffe über diese Arbeitsplatzrechner (bzw. Systeme) sowie die Kommu­nika­tion zwischen den Arbeitsplatzrechnern (bzw. Systeme) und den Systemen der CVC-Root-CA im geschützten Bereich geeignet gegen Manipulationen und un­autorisierte Nutzung geschützt werden und für diese Arbeitsplatzrechner (bzw. Systeme) das gleiche Sicherheitsniveau wie für die CVC-Root-CA eingehalten wird.

**⌫**

**⌦ TIP1-A\_5237 Sicherer Betrieb von Systemkomponenten der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS den sicheren Betrieb von Systemkompo­nen­ten gewährleisten. Hierzu MÜSSEN mindestens die folgenden Maßnahmen er­griffen wer­den: (a) Umsetzung einer Benutzerauthentisierung, die mindestens dem Sicher­heits­niveau eines Logins mit Username und Passwort entspricht, (b) Um­setzung einer Zugriffskontrolle, (c) Sichere Administration und Konfiguration von Kom­po­nen­ten, (d) Maßnahmen zur Systemhärtung, (e) Zeitnahes Einspielen von Updates, ins­besondere von Sicherheitsupdates, (f) Einsatz aktueller Virenschutz­pro­gramme.

**⌫**

**⌦ TIP1-A\_5372 Systemtechnische Trennung bei Aufbau und Betrieb der CVC-Root-CA**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass die CVC-Root-CA hinsichtlich der Signaturidentitäten vollständig getrennt von anderen Systemen und deren Signaturidentitäten aufgebaut und betrieben wird.

**⌫**

## Veröffentlichung von Informationen

**⌦ TIP1-A\_5238 Veröffentlichung des öffentlichen Root-Schlüssels**

Der Anbieter der CVC-Root-CA MUSS den öffentlichen Root-CA-Schlüssel auf einer sicheren Internet­seite zum Download zur Verfügung stellen.

**⌫**

**⌦ TIP1-A\_5239 Sicherstellung der Integrität und Authentizität des öffentlichen Schlüssels bei Veröffentlichung**

Der Anbieter der CVC-Root-CA MUSS die Integrität und Authentizität des auf den Internetseiten publizierten öffentlichen Schlüssels sicherstellen.

**⌫**

**⌦ TIP1-A\_5240 Bereitstellung des Fingerprints zum öffentlichen Schlüssel**

Der Anbieter der CVC-Root-CA MUSS einen Fingerprint des öffentlichen Schlüssels auf Anfrage per Briefpost zur Verfügung stellen.

**⌫**

**⌦ TIP1-A\_5241 Bereitstellung von Cross-Zertifikaten (Link-Zertifikaten)**

Im Falle eines Wechsels der Schlüsselversion MUSS die CVC-Root-CA das zuge­hörige Cross-CV-Zertifikat (Link-Zertifikat) auf den Internetseiten des Anbieters für einen Download zur Verfügung stellen. Im Falle eines planmäßigen Wechsels MUSS die CVC-Root-CA das Cross-Zertifikat spätestens bis zum 15. Oktober des vorherigen Jahres bereitstellen.

**⌫**

**⌦ TIP1-A\_5243 Information an die CVC-CAs über die Verfügbarkeit einer neuen Root-Version**

Der Anbieter der CVC-Root-CA MUSS die CVC-CAs der zweiten Ebene und den Anbieter des TSL-Dienstes über die Verfügbarkeit eines neuen öffentlichen Root-Schlüssels informieren.

**⌫**

## Verwaltung von Daten zur Zulassung und Registrierung

Der Anbieter der CVC-Root-CA speichert die von der gematik übergebenen Daten zur Zulassung von TSP-CVCs und Registrierung von CVC-CAs. Die aktuell verfügbaren Informationen werden bei Ausstellung eines CVC-CA-Zertifikats gegen die Antragsdaten geprüft.

**⌦ TIP1-A\_5245 Schnittstelle zur Einsicht und Übermittlung von Registrierungs­daten**

Der Anbieter der CVC-Root-CA MUSS der gematik und den beteiligten Akteuren eine Schnitt­stelle mit geeigneten Authentisierungsmechanismen zur Einsicht und Übermittlung von Registrierungsdaten anbieten.

**⌫**

Die Schnittstelle kann z.B. durch ein sicheres Web-Frontend realisiert werden.

**⌦ TIP1-A\_5246 Daten zum TSP-CVC**

Der Anbieter der CVC-Root-CA MUSS zu einem TSP-CVC die folgenden Daten ver­walten: (a) Ein­deutiger Name des TSP-CVC, (b) Stammdaten, (c) Registrierungs­datum, (d) Release- bzw. Versionsbezug, (e) Anzahl bereits ausgestellter CVC-CAs, (f) Limit maximal erlaubter auszustellender CVC-CAs, (g) Status der Registrierung, (h) CVC-Zugriffsprofile.

**⌫**

**⌦ TIP1-A\_5247 Daten zur CVC-CA**

Der Anbieter der CVC-Root-CA MUSS zu einer CVC-CA die folgenden Daten verwalten: (a) Eindeutiger Name der CVC-CA, (b) Vorgangsdaten, (c) CVC-CA-Zertifikat, (d) ausstellende CVC-Root-CA, (e) Status der CVC-CA.

**⌫**

## Unterscheidung Produktiv-CVC-Root-CA und Test-CVC-Root-CA

Bei der PKI für CV-Zertifikate wird zwischen einer Produktiv-PKI und einer Test-PKI unter­schieden.

**⌦ TIP1-A\_5248 Betrieb von Test-CVC-Root-CAs**

Der Anbieter der CVC-Root-CA MUSS neben einer Produktiv-CVC-Root-CA eben­falls eine Test-CVC-Root-CA betreiben.

**⌫**

Der Anbieter der CVC-Root-CA soll sicherstellen, dass das Testsystem von dem Pro­duk­tiv­­system technisch, organisatorisch und betrieblich so getrennt wird, dass keine ge­gen­­seitige Beeinflussung und keine Verwechslung möglich ist (vgl. [gem­Spec\_Sich\_DS#3.7]).

**⌦ TIP1-A\_5249 Backup und Verfügbarkeit der CVC-Root-CA für Produktiv- und Testumgebung**

Der Anbieter der CVC-Root-CA MUSS a) für die Verfügbarkeit der CVC-Root-CA mindestens ein dediziertes Backup-HSM (cold standby) vorhalten, das bei Ausfall eines HSM (Produktiv- oder Testumgebung) eingesetzt werden kann, b) für jede Betriebsumgebung ein separates Schlüssel-Backup der Root-CVC-CA nach den vom HSM-Hersteller vorgegebenen Backup-Verfahren sicher erstellen und sicher verwahren.

**⌫**

Der Prozess zur Ausgabe von „(Test-)CVC-CA-Zertifikaten“ ist für die Produktiv-CVC-Root-CA und für die Test-CVC-Root-CA identisch.

# 

# Funktionsmerkmale

## Ausstellung von CVC-CA-Zertifikaten durch die CVC-Root-CA

### Schnittstelle P\_Sub\_CA\_Certification\_CVC

Die Schnittstelle „P\_Sub\_CA\_Certification\_CVC“ ist eine organisatorische Schnittstelle zur Veranlassung der Ausstellung eines CVC-Sub-CA-Zertifikats für einen TSP-CVC durch die CVC-Root-CA, mit dem der TSP-CVC dann berechtigt ist, CV-Zertifikate für Smartcards der TI zu erzeugen (vgl. [gemKPT\_Arch\_TIP#5.7.4]).

Der TSP-CVC verfügt über eine Zulassung der gematik und hat die CVC-CA, für die er ein CVC-CA-Zertifikat beantragt, bei der gematik registriert. Die Informationen über die Zulassung und Registrierung wurden der CVC-Root-CA durch die gematik zur Verfügung gestellt.

Die Beantragung geschieht in den folgenden Schritten:

* Der TSP-CVC stellt einen schriftlichen Antrag bei der CVC-Root-CA.
* Nach erfolgreicher Prüfung des Antrags durch die CVC-Root-CA wird dem TSP-CVC ein Termin mitgeteilt, an dem ein Mitarbeiter des TSP-CVC das CVC-CA-Zertifikat persönlich bei der CVC-Root-CA abholen kann.
* An dem genannten Termin überbringt ein Mitarbeiter des TSP-CVC den CVC-PKCS#10-Request persönlich zur CVC-Root-CA.
* Nach erfolgreicher Prüfung des CVC-PKCS#10-Requests wird durch die CVC-Root-CA das neue CVC-CA-Zertifikat erstellt und an den Mitar­beiter des TSP-CVC übergeben.

#### Schnittstellendefinition

Die CVC-Root-CA erstellt auf der Grundlage eines erfolgreich geprüften Antrags eines TSP-CVC ein CVC-CA-Zertifikat sofern der TSP-CVC über eine Zulassung der gematik verfügt.

**⌦ TIP1-A\_5250 Schriftlicher Antrag auf Ausstellung eines CVC-CA-Zertifikats**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass ein schriftlicher Antrag des TSP-CVC zur Ausstellung eines CVC-CA-Zertifikats vorliegt.

**⌫**

**⌦ TIP1-A\_5251 Eingangsdaten zur Erzeugung eines CVC-CA-Zertifikats, die durch den TSP-CVC zur Verfügung gestellt werden**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass zur Ausstellung eines CVC-CA-Zertifi­kats mindestens die folgenden Eingangsdaten vorliegen: (a) Name und Anschrift der CVC-CA, (b) Name und Vorname einer Kontaktperson, (c) Typ des CVC-CA-Zertifikats (Test oder produktiv), (d) Öffentlicher Schlüssel, (e) Fingerprint über den öffentlichen Schlüssel, für den das CVC-CA-Zertifikat erzeugt werden soll, (f) Card Holder Referenz, CHR, bestehend aus der CAR zu dem Schlüssel der zertifiziert werden soll und (g) Unterschriften zweier hierfür berechtigter und bei der gematik registrierter Mitarbeiter des TSP-CVC.

**⌫**

**⌦ TIP1-A\_5252 CVC-PKCS#10-Request zur Erzeugung eines CVC-CA-Zertifikats**

Der Anbieter der CVC-Root-CA MUSS die Korrektheit des CVC-PKCS#10-Requests des TSP-CVC zur Ausstellung eines CVC-CA-Zertifikats verifizieren.

**⌫**

Für die Erstellung des CVC-CA-Zertifikats werden die durch den TSP-CVC zur Verfügung gestellten Eingangsdaten sowie durch die CVC-Root-CA zu bestimmende Parameter verwendet (z.B. Certification Authority Reference (CAR) oder Certificate Effective Date (CED) und Certificate Expiration Date (CXD) bei Ausstellung eines CVC-CA-Zertifikats der Kartengeneration 2).

**⌦ TIP1-A\_5253 Übergabe des CVC-CA-Zertifikats an den TSP-CVC**

Der Anbieter der CVC-Root-CA MUSS das erzeugte CVC-CA-Zertifikat an den TSP-CVC überge­ben.

**⌫**

#### Umsetzung

Die CVC-Root-CA erhält und prüft den schriftlichen Antrag des TSP-CVC auf Ausstellung eines CVC-CA-Zertifikats.

**⌦ TIP1-A\_5254 Prüfung des schriftlichen Antrags auf Ausstellung eines CVC-CA-Zertifikats**

Der Anbieter der CVC-Root-CA MUSS den schriftlichen Antrag des TSP-CVC auf Ausstellung eines CVC-CA-Zertifikats prüfen. Der Anbieter der CVC-Root-CA MUSS prüfen, ob (a) Name und An­schrift des TSP-CVC korrekt sind, (b) eine Kontaktperson angegeben wurde, die im Rahmen der Zulassung (oder einer Änderung) der gematik benannt wurde und eine der Rollen "Leiter CA", "Sicherheitsbeauftragter" bzw. "Antragsteller CVC-CA-Zer­tifikat" inne hat, (c) der Antrag von zwei hierfür berechtigten Mitarbeitern des TSP-CVC unterschrieben wurde und eine der Unterschriften von einem Mitarbeiter stammt, dem die Rolle "Leiter CVC-CA" zugewiesen wurde und die zweite Unter­schrift von einem weiteren bei der Zulassung bzw. einer Änderungsmitteilung ge­nannten Mitarbeiter ("Sicherheitsbeauftragter" bzw. "Antragsteller CVC-CA-Zertifi­kat") stammt.

**⌫**

**⌦ TIP1-A\_5255 Ergebnis der Prüfung des schriftlichen Antrags auf Ausstellung eines CVC-CA-Zertifikats**

Der Anbieter der CVC-Root-CA MUSS das Ergebnis der Prüfung des schriftlichen Antrags doku­mentieren und den TSP-CVC über das Ergebnis schriftlich informieren.

**⌫**

**⌦ TIP1-A\_5256 Vereinbarung zur Übergabe des CVC-PKCS#10-Requests**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass nur nach einer erfolgreichen Prüfung des schriftlichen Antrags zwischen der CVC-Root-CA und dem TSP-CVC ein Termin für die persönliche Übergabe des CVC-PKCS#10-Requests und die Ausstellung CVC-CA-Zertifikates vereinbart wird.

**⌫**

Mit der persönlichen Übergabe des CVC-PKCS#10-Requests sind durch die CVC-Root-CA folgende Prüfungen vorzunehmen:

**⌦ TIP1-A\_5257 Prüfung des Mitarbeiters des TSP-CVC und dessen Berechtigung**

Der Anbieter der CVC-Root-CA MUSS prüfen, ob die Person, die den CVC-PKCS#10-Request überbringt, sich als Mitarbeiter des TSP-CVC ausweisen kann und diese durch den TSP-CVC zur persönlichen Übergabe des CVC-PKCS#10-Requests autorisiert wurde.

**⌫**

**⌦ TIP1-A\_5258 Prüfung des CVC-PKCS#10-Requests**

Der Anbieter der CVC-Root-CA MUSS die Korrektheit des CVC-PKCS#10-Requests prüfen. Der Anbieter der CVC-Root-CA MUSS prüfen, ob (a) die Signatur des CVC-PKCS#10-Requests mathe­matisch korrekt ist, (b) im Request-Feld certificationRequestInfo das Feld ver­sion den Wert 0 hat, (c) die Angaben im Feld algorithm aus dem RequestInfo-Feld subjectPKInfo und dem Feld algorithm aus dem Request-Feld signatureAlgo­rithm zueinander konsistent sind, (d) der im RequestInfo-Feld subjectPKInfo enthaltene öffentliche Schlüssel (Feld subjectPublicKey) zu dem im schriftlichen Antrag enthaltenen öffentlichen Schlüssel identisch ist.

**⌫**

**⌦ TIP1-A\_5259 Erstellung eines CVC-CA-Zertifikats**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass ein CVC-CA-Zertifikat nur dann erstellt wird, falls (a) der TSP-CVC über eine aktuell gültige Zulassung der gematik verfügt (b) die Prüfung des Mitarbeiters des TSP-CVC und dessen Berechtigung erfolgreich war, (c) die Prüfung des CVC-PKCS#10-Requests erfolgreich war, (d) die Prüfung des Fingerprints über den öffentlichen Schlüssel erfolgreich war (e) die Angabe des CHR im Feld subject aus dem Request-Feld certificationRequestInfo eindeutig ist und (f) der in der CHR enthaltene CA-Name für die Kartengeneration eindeutig ist.

**⌫**

Für die Belegung der Zertifikatsfelder bzw. zur Erzeugung des CVC-CA-Zertifikats sind durch die CVC-Root-CA die folgenden Anforderungen zu erfüllen:

**⌦ TIP1-A\_5260 Berücksichtigung von Eingangsdaten gemäß [gemSpec\_PKI] bei Ausstellung von CVC-CA-Zertifikaten**

Für die Erzeugung eines CVC-CA-Zertifikats MUSS die CVC-Root-CA sicherstellen, dass die Festlegungen gemäß der Spezifikation PKI der TI-Plattform [gem­Spec\_PKI] hinsichtlich der Zertifikatsprofile, der Object Identifier sowie der Ko­dierung von Identitäten berücksichtigt werden.

**⌫**

**⌦ TIP1-A\_5261 Verwendung der Eingangsdaten des TSP-CVC**

Der Anbieter der CVC-Root-CA MUSS zur Erzeugung eines CVC-CA-Zertifikats die vom TSP-CVC zur Verfügung gestellten Eingangsdaten aus dem CVC-PKCS#10-Request ver­wen­den.

**⌫**

**⌦ TIP1-A\_5262 Setzen der Certificate Authority Reference (CAR)**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass über die Felder Service-Indikator, CA-spe­zifische Informationen, Algorithmen-Referenz und Datum eine eindeutige Zu­ordnung zu der korrekten Root-Version gegeben ist.

**⌫**

**⌦ TIP1-A\_5263 Setzen des Datums in Certificate Authority Reference (CAR)**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass das Feld Datum der Certificate Authority Reference die beiden letzten Ziffern des Jahres enthält, in dem die CVC-Root-CA den Wechsel der Root-Version durchgeführt, d.h. den Schlüssel aktiviert, hat.

**⌫**

Die beiden letzten Ziffern des Jahres, die die CVC-Root-CA als Datum in ein CVC-CA-Zertifikat einer CVC-CA in das Feld CAR einträgt, beziehen sich auf das Jahr der Aktivierung des Schlüssels.

**⌦ TIP1-A\_5264 Setzen der Certificate Effective Date (CED)**

Der Anbieter der CVC-Root-CA MUSS bei Erzeugung eines CVC-CA-Zertifikats für die Kartengeneration 2 das Erstellungsdatum in das Datenfeld CED eintragen.

**⌫**

**⌦ TIP1-A\_5265 Setzen der Certificate Expiration Date (CXD)**

Der Anbieter der CVC-Root-CA MUSS bei Erzeugung eines CVC-CA-Zertifikats für die Karten­ge­neration 2 als Certificate Expiration Date (CXD) ein Datum einstellen, das die Gül­tig­keitsdauer des CVC-CA-Zertifikats festlegt und die in Tab\_PKI\_801 definierten maximalen Gültigkeitsdauern einhält.

**⌫**

Tabelle 1: Tab\_PKI\_801 Maximale Gültigkeitsdauern von CVC-CA-Zertifikaten

| Kartentyp | Maximale Gültigkeitsdauer |
| --- | --- |
| eGK | 8 Jahre |
| HBA | 8 Jahre |
| SMC-B | 8 Jahre |
| HSM-B | 8 Jahre |
| SMC-K | 8 Jahre |
| SMC-KT | 8 Jahre |

**⌦ TIP1-A\_5266 Signierung des CVC-CA-Zertifikats durch die CVC-Root-CA**

Die zusammengestellten Daten für das CVC-CA-Zertifikat, das für einen Einsatz in der Produktivumgebung vorgesehen ist, MÜSSEN durch die Produktiv-CVC-Root-CA mit dem zugehörigen privaten Schlüssel signiert werden.

**⌫**

Das Signaturverfahren bzw. die Vorgaben an das Signaturformat sind in [gem­Spec\_Krypt#2.1.2] bzw. in [gemSpec\_PKI#6.7] festgelegt.

**⌦ TIP1-A\_5267 Protokollierung**

Der Anbieter der CVC-Root-CA MUSS den Antrag sowie das neu erstellte CVC-CA-Zertifikat in eine interne Zertifikatsprotokollierung übernehmen.

**⌫**

Die Inhalte dieser Protokollierung sollen einen revisionssicheren Nachweis über das ordnungsgemäße Arbeiten der CVC-Root-CA ermöglichen. Sie stellen keinen Verzeichnisdienst dar, über den Dritte CVC-CA-Zertifikate abrufen können.

### Artefakte

#### CVC-PKCS#10-Request

Der TSP-CVC erstellt über den öffentlichen Schlüssel einen CVC-PKCS#10-Request gemäß der Struktur nach [RFC2986]. Dieser wird durch den TSP-CVC mit dem zuge­hörigen privaten Schlüssel signiert.

**⌦ TIP1-A\_5268 CVC-PKCS#10-Request, Format des technischen Requests**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass die technische Bearbeitung eines CVC-CA-Zertifikats durch einen CVC-PKCS#10-Request gemäß der Struktur nach [RFC2986] erfolgt.

**⌫**

**⌦ TIP1-A\_5269 CVC-PKCS#10-Request, Konkretisierungen für die Karten­ge­neration 1**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass für die Beantragung eines CVC-CA-Zertifikats der Kartengeneration 1 folgende Konkretisierungen zu [RFC2986] durch den TSP-CVC vorgenommen wurden: (a) Im Request-Feld certificationRequest­Info muss version den Wert 0 haben. (b) Im Request-Feld certificationRequest­Info muss subject die notwendigen Inhalte des CV-Zertifikats enthalten. Für die An­gabe der Attribute müssen die OIDs gemäß Tab\_PKI\_802 verwendet werden. (c) Im RequestInfo-Feld subjectPKInfo muss algorithm den Verwendungszweck rsaEn­crytion ([PKCS#1], OID 1.2.840.113549.1.1.1) angeben. (d) Im Request-Feld sig­na­tureAlgorithm muss algorithm das Signaturverfahren sha256WithRSAEn­cryption ([PKCS#1], OID 1.2.840.113549.1.1.11) angeben.

**⌫**

**⌦ TIP1-A\_5270 CVC-PKCS#10-Request, Konkretisierungen für die Kartengene­ration 2**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass für die Beantragung eines CVC-CA-Zertifikats der Kartengeneration 2 folgende Konkretisierungen zu [RFC2986] durch den TSP-CVC vorgenommen wurden: (a) Im Request-Feld certificationRequest­Info muss version den Wert 0 haben. (b) Im Request-Feld certificationRequest­Info muss subject die notwendigen Inhalte des CV-Zertifikats enthalten. Für die An­gabe der Attribute müssen die OIDs gemäß Tab\_PKI\_803 verwendet werden. (c) Im RequestInfo-Feld subjectPKInfo muss subjectPublicKey den Domainparameter (Punkt Q des öffentlichen Schlüssels eines CV-Zertifikats der Kartengeneration 2; brainpoolP256r1, brainpoolP384r1 oder brainpoolP512r1) enthalten. (d) Im Request­Info-Feld subjectPKInfo muss algorithm den Verwendungszweck ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2), ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3) oder ecdsa-with-SHA512 (OID 1.2.840.10045.4.3.4) angeben. (e) Im Request-Feld signatureAlgorithm muss algorithm das Signaturverfahren ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2), ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3) oder ecdsa-with-SHA512 (OID 1.2.840.10045.4.3.4) angeben.

**⌫**

Die Angabe von Parametern (subjectPKInfo) bzw. die Verwendung des Signatur­ver­fahrens (signatureAlgorithm) sind durch den TSP-CVC konsistent zu belegen bzw. an­zu­wen­den. D.h. die Verwendung von brainpoolP256r1 (brainpoolP384r1 bzw. brain­poolP512r1) bedingt die Nutzung von ecc-with-sha256 (ecc-with-sha384 bzw. ecc-with-sha512) und ecdsa-with-SHA256 (ecdsa-with-SHA384 bzw. ecdsa-with-SHA512). Eine diesbezügliche Konsistenzprüfung wird durch die CVC-Root-CA im Rahmen der Um­setzung vorgenommen (vgl. [TIP1-A\_5258]).

**⌦ TIP1-A\_5271 CVC-PKCS#10-Request für Kartengeneration 1, Object Identifier der Attribute**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass für die Attribute der Kartengeneration 1 die folgenden Object Identifier verwendet werden:

id-cvc-attributes OBJECT IDENTIFIER ::= {

iso(1) identified-organization(3) dod(6) internet(1)

private(4) enterprise(1) D-Trust GmbH(4788) 4

}

id-cvc-certificateProfileIdentifier OBJECT IDENTIFIER ::= {

id-cvc-attributes 1

}

id-cvc-certificateHolderReference OBJECT IDENTIFIER ::= {

id-cvc-attributes 2

}

id-cvc-CHR-cAName OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 1

}

id-cvc-CHR-serviceIndicator OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 2

}

id-cvc-CHR-keyDicretionaryData OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 3

}

id-cvc-CHR-algorithmReference OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 4

}

id-cvc-CHR-yearofActivation OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 5

}

id-cvc-algorithmIdentifier OBJECT IDENTIFIER ::= {

id-cvc-attributes 4

}

**⌫**

In der folgenden Tabelle 2 sind die OIDs der Attribute zwecks leichterer Verständlichkeit in tabellarische Ansicht mit Inhaltsbeschreibung dargestellt:

Tabelle 2: Tab\_PKI\_802 OID der Attribute im CVC-PKCS#10-Request für Kartengeneration 1

| OID | | | | | | | | | | | Name bzw. Inhalt der OID |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  |  |  |  |  |  |  |  |  |  | iso |  |
|  | 3 |  |  |  |  |  |  |  |  |  | identified-organization |  |
|  |  | 6 |  |  |  |  |  |  |  |  | dod |  |
|  |  |  | 1 |  |  |  |  |  |  |  | internet |  |
|  |  |  |  | 4 |  |  |  |  |  |  | private |  |
|  |  |  |  |  | 1 |  |  |  |  |  | enterprise |  |
|  |  |  |  |  |  | 4788 |  |  |  |  | D-Trust GmbH |  |
|  |  |  |  |  |  |  | 4 |  |  |  | CVC-Attributes |  |
|  |  |  |  |  |  |  |  | 1 |  |  | CPI (Certificate Profile Identifier) (1 Byte hex) |  |
|  |  |  |  |  |  |  |  | 2 |  |  | CHR (Certificate Holder Reference) |  |
|  |  |  |  |  |  |  |  |  | 1 |  | CA-Name (5 Zeichen ASCII) |  |
|  |  |  |  |  |  |  |  |  | 2 |  | Service Indicator (1 nibble hex) |  |
|  |  |  |  |  |  |  |  |  | 3 |  | Discretionary Data (1 nibble hex) |  |
|  |  |  |  |  |  |  |  |  | 4 |  | Algorithm Reference (1 Byte hex) |  |
|  |  |  |  |  |  |  |  |  | 5 |  | Aktivierungsjahr (1 Byte hex) |  |
|  |  |  |  |  |  |  |  | 4 |  |  | OID (7 Byte hex für CAs) |  |

Anmerkung: Im Gegensatz zu den CVC-CA-Zertifikaten für die Kartengeneration G0 der eGK ist das Attribut CHA in CVC-CA-Zertifikaten in der CVC-PKI für die Kartengeneration G1 der eGK nicht mehr enthalten.

Zur Unterscheidung der CV-Zertifikate der unterschiedlichen Kartengenerationen auch im Zertifikats-Request werden für die Requests für Kartengeneration 2 eigene Object Identifier festgelegt.

**⌦ TIP1-A\_5367 CVC-PKCS#10-Request für Kartengeneration 2, Object Identifier der Attribute**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass für die Attribute der Kartengeneration 2 die folgenden Object Identifier verwendet werden:

id-cvc-attributes OBJECT IDENTIFIER ::= {

iso(1) member-body(2) de(276) din-certco(0) gesundheitswesen(76)

instanzen-identifikatoren(3) organisationen(1) gematik(91) 44

}

id-cvc-certificateHolderReference OBJECT IDENTIFIER ::= {

id-cvc-attributes 2

}

id-cvc-CHR-cAName OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 1

}

id-cvc-CHR-serviceIndicator OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 2

}

id-cvc-CHR-keyDicretionaryData OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 3

}

id-cvc-CHR-algorithmReference OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 4

}

id-cvc-CHR-yearofActivation OBJECT IDENTIFIER ::= {

id-cvc-certificateHolderReference 5

}

}

**⌫**

In der folgenden Tabelle 3 sind die OIDs der Attribute zwecks leichterer Verständlichkeit in tabellarische Ansicht mit Inhaltsbeschreibung dargestellt:

Tabelle 3: Tab\_PKI\_803 OID der Attribute im CVC-PKCS#10-Request für Kartengeneration 2

| OID | | | | | | | | | | | Name bzw. Inhalt der OID |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 276 | 0 | 76 | 3 | 1 | 91 |  |  |  | gematik |  |
|  |  |  |  |  |  |  |  | 44 |  |  | CVC-Attributes |  |
|  |  |  |  |  |  |  |  |  | 2 |  | CHR (Certificate Holder Reference) |  |
|  |  |  |  |  |  |  |  |  |  | 1 | CA-Name (5 Zeichen ASCII) |  |
|  |  |  |  |  |  |  |  |  |  | 2 | Service Indicator (1 nibble hex) |  |
|  |  |  |  |  |  |  |  |  |  | 3 | Discretionary Data (1 nibble hex) |  |
|  |  |  |  |  |  |  |  |  |  | 4 | Algorithm Reference (1 Byte hex) |  |
|  |  |  |  |  |  |  |  |  |  | 5 | Aktivierungsjahr (1 Byte hex) |  |

Anmerkung: Gegenüber dem Zertifikatsrequest für CV-CA-Zertifikate der Kartengeneration 1 ergeben sich eine Reihe von Änderungen:

* CPI: nicht erforderlich, da für G2 ein fester Wert definiert ist
* CHAT: entspricht inhaltlich dem CHA aus G1 und wird per Konfiguration gemäß gematik- und Sektorzulassung von der CVC-Root gesetzt.
* CED und CXD: neu hinzugekommen; die Werte werden durch die CVC-Root-CA gemäß der hinterlegten Konfigurationsdaten festgelegt und sind somit kein Bestandteil des Zertifikatsrequests
* OID: gibt an für welchen Zweck die Schlüssel verwendet werden; die CVC-Root-CA wird gemäß der hinterlegten Konfigurationsdaten und übergreifend festgelegten zu verwendenden Krypto-Algorithmen einen festen Wert (nur abhängig von der tatsächlich verwendeten Schlüssellänge) eintragen, somit ist „OID“ kein Bestandteil des Zertifikatsrequests

**⌦ TIP1-A\_5272 CVC-PKCS#10-Request, Angabe der Attribute**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass CV-CA-Zertifikate nur für Requests mit den vollständigen und korrekten Attributwerten im subject des certificationRequestInfo ausgestellt werden.

**⌫**

Vorgaben für die einzelnen Werte der in Tabelle 2, bzw. Tabelle 3 angegebenen CVC-Attribute CPI, CHR, CA-Name, Service-Indikator, Discretionary Data, Algorithmenreferenz, Aktivierungsjahr und OID sind in [gemSpec\_PKI#6.4.1] bzw. in [gem­Spec\_PKI#6.7.2] festgelegt.

**⌦ TIP1-A\_5273 CVC-PKCS#10-Request, Kodierung**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass nur base-64 codierte CVC-PKCS#10-Request verarbeitet werden.

**⌫**

### Testunterstützung

Das Vorgehen bei der Erzeugung von CVC-CA-Zertifikaten ist für die Produktiv-CVC-Root-CA und für die Test-CVC-Root-CA identisch. Mit dem Antrag muss der TSP-CVC jedoch angeben, dass ein Test-CVC-CA-Zertifikat erzeugt werden soll und der Anbieter der CVC-Root-CA muss zur Erzeugung des CVC-CA-Zertifikats eine Test-CVC-Root-CA einsetzen.

**⌦ TIP1-A\_5274 Signierung des Test-CVC-CA-Zertifikats durch die Test-CVC-Root-CA**

Die zusammengestellten Daten für das Test-CVC-CA-Zertifikat MÜSSEN durch die Test-CVC-Root-CA mit dem zugehörigen privaten Schlüssel signiert werden.

**⌫**

## Informationen zur Zulassung und Registrierung von TSP-CVC

Die Prozesse zur Zulassung eines TSP-CVC und Registrierung einer durch den TSP-CVC betriebenen CVC-CA werden nicht durch den technischen Betreiber der CVC-Root-CA durchgeführt. Diese Prozesse werden durch die gematik vorgenommen. Die CVC-Root-CA erhält in regelmäßigen Abständen von der gematik die Informationen über zuge­las­sene und registrierte TSP-CVC bzw. CVC-CAs. Hierzu zählen ebenfalls Angaben über zurückgezogene Zulassungen. Diese Informationen werden durch die CVC-Root-CA nachgehalten und bei Ausstellung eines CVC-CA-Zertifikats geprüft.

Aus Sicht der CVC-Root-CA ergeben sich die im Folgenden beschriebenen Anfor­derungen.

**⌦ TIP1-A\_5275 Entgegennahme der Informationen zur Zulassung und Regis­trierung**

Der Anbieter der CVC-Root-CA MUSS die von gematik zur Verfügung gestellten Informationen hinsichtlich der Zulassung von TSP-CVC und der Registrierung von CVC-CAs entgegennehmen, den Empfang an die gematik authentisch und integer innerhalb eines Werktages bestätigen und vorhalten.

**⌫**

In einer CA-Datenbank der CVC-Root-CA werden alle relevanten Informationen der erfolgreich zugelassenen und registrierten CVC-CAs gespeichert. Bei Eingang eines Antrags auf die Ausstellung eines CVC-CA-Zertifikats wird auf Basis der vorgehaltenen Informationen verifiziert, ob der TSP-CVC zugelassen und die CVC-CA registriert wurde (vgl. Kapitel 6.1.1.2).

**⌦ TIP1-A\_5276 Protokollierung der Entgegennahme der Informationen zur Zulassung und Registrierung**

Der Anbieter der CVC-Root-CA MUSS die Entgegennahme von bereitgestellten Informationen hinsichtlich der Zulassung von TSP-CVC und der Registrierung von CVC-CAs sowie deren Vorhaltung (Aktualisierung der verfügbaren Informationen) protokollieren.

**⌫**

# 

# Anhang A – Verzeichnisse

## A1 – Abkürzungen

| **Kürzel** | **Erläuterung** |
| --- | --- |
| C2C | Card to Card |
| CA | Certification Authority |
| CAR | Certificate Authority Reference |
| CED | Certificate Effective Date |
| CHA | Certificate Holder Authorisation |
| CHAT | Certificate Holder Authorisation Template |
| CHR | Certificate Holder Reference |
| CPI | Certificate Profile Identifier |
| CV | Card Verifiable |
| CVC | Card Verifiable Certificate |
| CVC-CA | CA der zweiten Ebene der PKI für CV-Zertifikate |
| CVC-Root-CA | CA der obersten Ebene der PKI für CV-Zertifikate |
| CXD | Certificate Expiration Date |
| eGK | Elektronische Gesundheitskarte |
| gSMC | Gerätebezogene Security Module Card |
| gSMC-K | Gerätebezogene Security Module Card Konnektor als <holder> |
| gSMC-KT | Gerätebezogene Security Module Card Kartenterminal als <holder> |
| HBA | Heilberufsausweis |
| HSM | Hardwaresicherheitsmodul |
| OID | Object Identifier |
| PKI | Public Key Infrastructure |
| RFC | Request For Comment |
| RSA | Algorithmus benannt nach Rivest, Shamir und Adleman |
| SHA | Secure Hash Algorithm |
| SM-B | Sicherheitsmodul vom Typ B |
| SMC | Security Module Card |
| SMC-B | SMC vom Typ B |

## A2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

## A3 – Abbildungsverzeichnis

[Abbildung 1: Karten mit CV-Zertifikaten unter verschiedenen CVC-Root-CAs 7](#_Toc480468188)

[Abbildung 2: Beispielhafter Aufbau der CV-Hierarchie 8](#_Toc480468189)

[Abbildung 3: Nachbarsysteme der CVC-Root-CA 11](#_Toc480468190)

## A4 – Tabellenverzeichnis

[Tabelle 1: Tab\_PKI\_801 Maximale Gültigkeitsdauern von CVC-CA-Zertifikaten 30](#_Toc480468192)

[Tabelle 2: Tab\_PKI\_802 OID der Attribute im CVC-PKCS#10-Request für Kartengeneration 1 32](#_Toc480468193)

[Tabelle 3: Tab\_PKI\_803 OID der Attribute im CVC-PKCS#10-Request für Kartengeneration 2 33](#_Toc480468194)

## A5 - Referenzierte Dokumente

### A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegen­den Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

| **[Quelle]** | **Herausgeber: Titel** |
| --- | --- |
| [gemGlossar] | gematik: Glossar der Telematikinfrastruktur |
| [gemKPT\_Arch\_TIP] | gematik: Konzept Architektur der TI-Plattform |
| [gemKPT\_PKI\_TIP] | gematik: Konzept PKI der TI-Plattform |
| [gemRL\_Betr\_TI | gematik: Übergreifende Richtlinien zum Betrieb der Ti |
| [gemSpec\_CVC\_TSP] | gematik: Spezifikation - Trust Service Provider CVC |
| [gemSpec\_Krypt] | gematik: Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur |
| [gemSpec\_PKI] | gematik: Übergreifende Spezifikation – Spezifikation PKI |
| [gemSpec\_SiBetrUmg] | gematik: Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI |
| [gemSpec\_Sich\_DS] | gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen |

### A5.2 – Weitere Dokumente

|  |  |
| --- | --- |
| **[Quelle]** | **Herausgeber (Erscheinungsdatum): Titel** |
| [PKCS#1] | RSA Laboratories (June 14, 2002): RSA Cryptography Standard v2.1  (earlier versions: V1.5: Nov. 1993, V2.0: July, 1998) |
| [RFC2119] | RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt |
| [RFC2986] | RFC 2986 (November 2000): PKCS #10: Certification Request Syntax Specification, Version 1.7 Nystrom, M.; Kaliski, B. |