Einführung der Gesundheitskarte

Spezifikation

Trust Service Provider CVC

|  |  |
| --- | --- |
| Version: | 1.8.1 |
| Revision: | \main\rel\_online\rel\_ors1\rel\_opb1\75 |
| Stand: | 21.04.2017 |
| Status: | freigegeben |
| Klassifizierung: | öffentlich |
| Referenzierung: | [gemSpec\_CVC\_TSP] |

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung lt. Änderungsliste

Dokumentenhistorie

| **Version** | | **Stand** | **Kap./ Seite** | **Grund der Änderung, besondere Hinweise** | | **Bearbeitung** |
| --- | --- | --- | --- | --- | --- | --- |
| 0.5.0 | | 26.07.12 |  | zur Abstimmung freigegeben | | PL P77 |
| 1.0.0 | | 15.10.12 |  | Einarbeitung Kommentierung Gesellschafter | | gematik |
| 1.1.0 | | 12.11.12 |  | | Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung | gematik |
| 1.2.0 | | 06.06.13 |  | | Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen), Kommentierung Gesamtpaket | gematik |
| 1.3.0 | 18.12.13 | |  | | Einarbeitung Kommentare Änderungsliste | gematik |
| 1.4.0 | 21.02.14 | |  | | Losübergreifende Synchronisation | gematik |
| 1.5.0 | 17.04.14 | |  | | Die Anforderung TIP-A-2692 wurde neu formuliert | gematik |
| 1.5.9 | 18.12.15 | |  | | Anpassungen zum Online-Produktivbetrieb (Stufe 1) | gematik |
| 1.6.0 RC | 16.03.16 | |  | | Zur Freigabe empfohlen | gematik |
| 1.6.0  RC B | 02.05.16 | |  | | Einarbeitung weitere GKV-SV-Kommentierung | gematik |
| 1.6.1 | 26.05.16 | |  | | freigegeben | gematik |
| 1.7.0 | 24.08.16 | |  | | Einarbeitung weiterer Kommentare | gematik |
| 1.8.0 | 28.10.16 | |  | | Aufnahme SMC-B für Organisationen der Gesellschafter, Anpassungen gemäß Änderungsliste | gematik |
|  | 21.04.17 | |  | | P.14.9 | gematik |
| 1.8.1 | 21.04.17 | |  | | freigegeben | gematik |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 5](#_Toc486426787)

[1.1 Zielsetzung 5](#_Toc486426788)

[1.2 Zielgruppe 5](#_Toc486426789)

[1.3 Geltungsbereich 5](#_Toc486426790)

[1.4 Abgrenzungen 5](#_Toc486426791)

[1.5 Methodik 6](#_Toc486426792)

[1.6 Unterscheidung der Anforderungsadressaten 6](#_Toc486426793)

[2 Systemüberblick 7](#_Toc486426794)

[2.1 Hierarchie der PKI für CV-Zertifikate 7](#_Toc486426795)

[2.2 Begriffsverwendung 7](#_Toc486426796)

[3 Systemkontext 9](#_Toc486426797)

[3.1 Akteure und Rollen 9](#_Toc486426798)

[3.1.1 Anbieter der CVC-Root-CA 9](#_Toc486426799)

[3.1.2 Kartenherausgeber 10](#_Toc486426800)

[3.1.3 TSP-CVC 10](#_Toc486426801)

[3.1.4 Kartenpersonalisierer 11](#_Toc486426802)

[3.1.5 Zertifikatsnehmer 11](#_Toc486426803)

[3.1.5.1 Karteninhaber (eGK) 11](#_Toc486426804)

[3.1.5.2 Karteninhaber (HBA, SM-B für medizinische Institutionen oder Kostenträger) 11](#_Toc486426805)

[3.1.5.3 Karteninhaber (gSMC, SM-B für Gesellschafterorganisationen) 12](#_Toc486426806)

[3.2 Nachbarsysteme 12](#_Toc486426807)

[3.3 Zugriffsprofile 13](#_Toc486426808)

[3.4 Sperren und Nachladen von CV-Zertifikaten der Karten- generation 2 14](#_Toc486426809)

[4 Übergreifende Festlegungen 15](#_Toc486426810)

[4.1 Erstellung Ausgabepolicy durch TSP-CVC 15](#_Toc486426811)

[4.2 Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-CVC 15](#_Toc486426812)

[4.3 Zulassung 16](#_Toc486426813)

[4.4 Registrierung und Qualifizierung 16](#_Toc486426814)

[4.5 Zusammenspiel Kartenherausgeber, CVC-CA und Kartenpersonalisierer 18](#_Toc486426815)

[4.6 Mindestanforderungen an eine CVC-CA 21](#_Toc486426816)

[4.6.1 Schutzbedarfsfeststellung 21](#_Toc486426817)

[4.6.2 Verfügbarkeit der CVC-CA 22](#_Toc486426818)

[4.6.3 Ausschließlichkeit und Dauer der Schlüsselnutzung 22](#_Toc486426819)

[4.6.4 Verlust der Zulassung 23](#_Toc486426820)

[4.6.5 Sicherheit des Schlüsselpaares 23](#_Toc486426821)

[4.6.6 Algorithmen und Schlüssellängen 27](#_Toc486426822)

[4.6.7 Schlüsselversionen 27](#_Toc486426823)

[4.6.8 Protokollierung 28](#_Toc486426824)

[4.6.9 Personelle Anforderungen 30](#_Toc486426825)

[4.6.10 Betriebliche Anforderungen 31](#_Toc486426826)

[4.6.11 Authentizität des öffentlichen Schlüssels der CVC-CA 32](#_Toc486426827)

[4.6.12 Synchronisierung mit dem Zeitdienst 32](#_Toc486426828)

[4.7 Beantragung eines CV-Zertifikats für die CVC-CA 33](#_Toc486426829)

[4.8 Unterscheidung produktiver CVC-CA und Test-CVC-CA 35](#_Toc486426830)

[5 Funktionsmerkmale 37](#_Toc486426831)

[5.1 Ausstellung von CV-Kartenzertifikaten durch CVC-CA 37](#_Toc486426832)

[5.1.1 Schnittstelle P\_CVC\_Provisioning 37](#_Toc486426833)

[5.1.1.1 Schnittstellendefinition 37](#_Toc486426834)

[5.1.1.2 Umsetzung 39](#_Toc486426835)

[5.1.2 Artefakte 40](#_Toc486426836)

[5.1.2.1 Card Holder Reference 40](#_Toc486426837)

[5.1.2.2 Card Holder Authorization 40](#_Toc486426838)

[5.1.2.3 Certificate Authority Reference 41](#_Toc486426839)

[5.1.2.4 Datenobjekte eines CV-Zertifikats der Generation 2 41](#_Toc486426840)

[5.1.3 Testunterstützung 41](#_Toc486426841)

[6 Anhang A – Verzeichnisse 42](#_Toc486426842)

[6.1 A1 – Abkürzungen 42](#_Toc486426843)

[6.2 A2 – Glossar 43](#_Toc486426844)

[6.3 A3 – Abbildungsverzeichnis 43](#_Toc486426845)

[6.4 A4 – Tabellenverzeichnis 43](#_Toc486426846)

[~~6.5~~ A5 ~~-~~ Referenzierte Dokumente 43](#_Toc486426847)

[6.5.1 A5.1 – Dokumente der gematik 43](#_Toc486426848)

[6.5.2 A5.2 – Weitere Dokumente 44](#_Toc486426849)

# Einordnung des Dokumentes

## Zielsetzung

Die vorliegende Spezifikation definiert fachliche, betriebliche und personelle Anforderun­gen an den Produkttyp Trust Service Provider CVC (TSP-CVC) und stellt darüber hinaus Sicherheitsanforderungen hinsichtlich Konzeption und Betrieb einer CVC-CA. Es werden übergreifende Festlegungen sowie Anforderungen an die Schnittstellen zum Erhalt eines CVC-CA-Zertifikates durch die CVC-Root-CA bzw. zur Ausgabe von CV-Zertifikaten an einen Kartenherausgeber oder an einen von ihm benannten Dritten beschrieben.

## Zielgruppe

Das Dokument ist maßgeblich für Trust Service Provider CVC, Anbieter einer CVC-CA sowie Kartenpersonalisierer und Kartenherausgeber.

## 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

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zu den Themen­be­reichen

* CVC-Root-CA sowie
* Darstellung der Prozesse zur Zulassung und Registrierung eines TSP-CVC.

## 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.

## Unterscheidung der Anforderungsadressaten

Dieses Dokument enthält Anforderungen, welche sich an unterschiedliche Kartentypen richten. Dabei unterscheiden sich die Adressaten dieser Anforderungen je nach Kartentyp. Daher wird der Adressat generisch als *Herausgabeverantwortlicher* bezeichnet und dieser Begriff für die unterschiedlichen Kartentypen wie folgt definiert:

* Für eGK: Kartenherausgeber und Kartenpersonalisierer
* Für HBA/SMC-B: Kartenherausgeber oder ein von ihm benannter Dritter (zum Beispiel TSP-CVC)
* Für Gerätekarten (gSMC-K und -KT): Gerätehersteller (Konnektor-/Kartenterminal-Hersteller)[[1]](#footnote-2)

# 

# Systemüberblick

## Hierarchie der PKI für CV-Zertifikate

Für die CV-Zertifikate, die im Rahmen der Telematikinfrastruktur zum Einsatz kommen, wird eine CVC-PKI mit zweistufiger CA-Hierarchie umgesetzt (vgl. [gem­KPT\_PKI\_TIP#5.2]). Die spezifischen CV-Zertifikate, die in einer eGK, einem HBA oder in einem Sicherheitsmodul (SM-B, gSMC) eingebracht werden, werden dabei durch einen Trust Service Provider für CV-Zertifikate (TSP-CVC) erzeugt. In der Hierarchie für CV-Zertifikate ist der TSP-CVC eine CA der zweiten Ebene, er wird im Folgenden auch mit „CVC-CA“ bezeichnet. Die CV-Zertifikate des TSP-CVC werden durch die über­geordnete CVC-Root-CA erzeugt und durch diese verteilt.

Für die Kartengeneration 2 werden die CV-Zertifikate auf ECC-basierte Kryptographie um­gestellt werden. Eine Cross-Zertifizierung, die üblicherweise benutzt wird, um die Ver­bindung zwischen zwei Zertifizierungsstellen herzustellen, kann nicht ohne Weiteres technologieübergreifend zwischen RSA-basierten und ECC-basierten Zer­tifi­katen genutzt werden. Daher ist auch eine eigene, separate CVC-PKI für Karten­generation 2 mit einer zweiten, separaten CVC-Root-CA notwendig.

Die Grundlagen und die Hierarchie der PKI für CV-Zertifikate sind in [gem­KPT\_PKI\_TIP#5] beschrieben. Das zugehörige Vertrauensmodell wird dort ebenfalls er­läutert. Anforderungen an die Zertifikatsprofile sowie an die Prüfung von CV-Zertifikaten sind in [gemSpec\_PKI] in den Kapiteln 6.4 und 6.7 (Zertifikatsprofile) sowie in 8.7 und 8.8 (Zertifikatsprüfung) beschrieben.

Die Funktion einer CVC-CA kann beispielsweise von Kartenpersonalisierern, TSP-X.509 oder den Karten­heraus­ge­bern selber übernommen werden. Diese CAs der zweiten Ebene arbeiten immer im Auf­trag der für die Kartenherausgabe verantwortlichen Organisation [gem­KPT\_PKI\_TIP#5.1].

Die gematik gibt im Rahmen ihrer Verantwortung für die PKI der CV-Zertifikate Min­destanforderungen an die Sicherheit, die Organisation und den Betrieb einer CVC-CA vor. Voraussetzung für das Ausstellen eines CV-Zertifikates für eine CVC-CA durch die CVC-Root-CA ist eine vorherige Zulassung des TSP-CVC und Registrierung seiner CVC-CA bei der gematik [gemKPT\_PKI\_TIP#7.2.2]. Im Rahmen seiner Zulassung muss der TSP-CVC die Einhaltung der Mindestanforderungen nachweisen. Nur zugelassene TSP dürfen CV-Zertifikate ausstellen.

Bei der PKI für CV-Zertifikate wird für jede Kartengeneration (Kartengeneration 1 und 2) zwischen einer PKI für die Produktivumgebung und einer Test-PKI für die Test- und Referenzumgebung unterschieden.

## Begriffsverwendung

Die gSMC kann in den technischen Ausprägungen gSMC-K als Sicherheitsmodul für den Konnektor und gSMC-KT als Sicherheitsmodul für das Kartenterminal vorliegen. In der weiteren Darstellung wird i.d.R. der Oberbegriff „gSMC“ verwendet. Eine Unterscheidung zwischen gSMC-K und gSMC-KT wird jedoch vorgenommen, wenn sie für die konkrete inhaltliche Betrachtung relevant ist.

Im Dokument wird der Begriff SMC-B (HSM-B) verwendet, um damit die Ausprägung des Sicherheitsmoduls als Karte (Hardwaresicherheitsmodul) zu beschreiben. Das HSM-B kann in Szenarien zum Einsatz kommen, in denen die Performance von Chipkarten nicht ausreichend ist, bspw. in Krankenhäusern. Funktional muss ein HSM-B vollständig einer SMC-B entsprechen. Als Oberbegriff wird die Bezeichnung SM-B bzw. Sicherheitsmodul vom Typ B benutzt. Eine Unterscheidung zwischen SMC-B und HSM-B wird jedoch vorgenommen, wenn sie für die konkrete inhaltliche Betrachtung relevant ist.

Weiterhin wird im Folgenden immer der Begriff „Chipkarte“ verwendet, unabhängig davon, ob es sich um eine Karte handelt oder um ein HSM. Eine Differenzierung wird jedoch ge­troffen, sofern dies für die inhaltliche Betrachtung erforderlich ist.

# 

# Systemkontext

## Akteure und Rollen

An der PKI für CV-Zertifikate können verschiedene Organisationen bzw. Personen beteiligt sein. In den folgenden Abschnitten wird ein Überblick über die vorhandenen Rollen (im Rah­men der PKI) und deren Zuständigkeiten bzw. Verantwortlichkeiten in Bezug auf die PKI für CV-Zertifikate gegeben.

Bei der folgenden Beschreibung wird von einer Trennung der Organisationen bzw. Per­so­nen bei der Ausübung der Rollen ausgegangen. Eine Organisation bzw. Person kann jedoch mehrere Rollen übernehmen.

Die Kartenherausgeber-Organisation als verantwortliche Stelle kann somit sämtliche Schritte der Kartenausgabe selbst ausführen und in den entsprechenden Rollen auftreten. Sie kann aber auch alle technischen Aufgaben und damit verbundenen organisatorischen Abläufe an einen von ihr benannten Dritten übertragen.

Übernimmt eine Organisation/Person eine Rolle, so kann sie Teile der zu dieser Rolle ge­hörenden Zuständigkeiten/Aufgaben an eine andere Organisation/Person übergeben. Hier­von unabhängig bleiben aber die im Folgenden genannten Verantwortlichkeiten bei der die Rolle ausübenden Organisation/Person.

Akteure und Rollen sind im Konzept PKI der TI-Plattform beschrieben [gem­KPT\_PKI\_TIP#2.7]. Hierzu gehören:

* TSP,
* Kartenherausgeber,
* Zertifikatsantragsteller,
* Zertifikatsnehmer und
* gematik.

Im Folgenden werden spezifische Ergänzungen aus Sicht der PKI für CV-Zertifikate dar­gestellt.

### 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 generiert wird, falls der TSP-CVC aktuell gültig durch die gematik zugelassen und registriert ist und, sofern erforderlich, eine Qualifizierung für diese CVC-CA vorliegt und
* das Ausstellen eines CVC-CA-Zertifikats gemäß den Vorgaben aus Kapitel 4.7 geschieht.

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

### Kartenherausgeber

Der Begriff des Kartenherausgebers wird in [gemGlossar] definiert. Siehe dazu auch [gemKPT\_PKI\_TIP#2.7.3].

Kartenherausgeber (Leistungserbringerorganisationen (LEOs), Kostenträger (KTR) und Gerätehersteller) sind für die Herausgabe von eGK, HBA, SMC-B, gSMC-K und gSMC-KT zuständig.

Der Kartenherausgeber muss, in Zusammenarbeit mit dem Kartenpersonalisierer und dem TSP-CVC, u.a. die korrekten Inhalte bzgl. Zugriffsprofil, ICCSN und öffentlichem Schlüs­sel sicherstellen. Die konkreten Anforderungen werden im Detail in Kapitel 4.5 gestellt.

Nach Ablauf der Gültigkeitsdauer einer Chipkarte muss ihre Einsetzbarkeit dauerhaft und nachweislich bezüglich der durch die CV-Zertifikate der Kartengeneration 1 geschützten Anwendungen unterbunden werden. Dies kann z. B. durch Einzug der Chipkarte durch den Karten­herausgeber oder durch Zerstören der Chipkarte durch den Karteninhaber realisiert werden. Das genaue Vorgehen wird durch den jeweiligen Kartenherausgeber in Policy-Dokumenten vorgegeben (vgl. [gemKPT\_PKI\_TIP#2.7.3]).

Sofern die Außerbetriebnahme durch den Einzug der Karte erfolgen soll, wird empfohlen, das Sicherheitsniveau so zu wählen, das es gleichwertig zur Protokollierung eingezogener und nicht eingezogener Karten ist. Die bereits etablierten Prozesse für die eGKs sind beizubehalten.

Eine mögliche Maßnahme kann bspw. die explizite Nachfrage beim Karteninhaber sein. Das genaue Vorgehen kann auch hier, wie bei Einzug bzw. Zerstörung der Chipkarte, durch den Kartenherausgeber vorgegeben werden.

Bei Einsatz von CV-Zertifikaten der Kartengeneration 2 kann auf die Außerbetriebnahme der Karte nach Ablauf ihrer Gültigkeit verzichtet werden, da somit das Gültigkeitsende der CV-Zertifikate erreicht wird und eine Zertifikatserneuerung nicht mehr vorgesehen ist.

Falls die zu den CV-Zertifikaten gehörenden Schlüsselpaare ihre Gültigkeit verlieren, gilt das gleiche, wie bei Ablauf der Gültigkeit der Chipkarte.

Sofern der Kartenherausgeber die entsprechenden Aufgaben ausgelagert hat, kann er seine Verantwortlichkeiten nur in Zusammenarbeit mit dem Kartenpersonalisierer und dem TSP-CVC erfüllen. Siehe dazu Abschnitte 3.1 und 4.5.

### TSP-CVC

Ein TSP-CVC ist für das Generieren der CV-Zertifikate für eine Chipkarte (eGK, HBA, SM-B, gSMC) zuständig. Dabei einzuhaltende Anforderungen werden durch dieses Dokument vorgegeben.

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

Falls CV-Rollen-Zertifikate erzeugt werden sollen, die ein Zugriffsprofil ungleich 0 (eGK) oder 8 (SM-B ohne Zugriff auf medizinische Daten) ent­halten (d. h. die für einen HBA bzw. für spezifische SM-B bestimmt sind), benötigt die CVC-CA hierfür eine Qualifizierung durch die jeweils zuständige Standesorganisation der Leistungs­erbringer. Die Anforderungen an diese Qualifizierung werden durch diese Standesorganisation geregelt. Die CVC-CA muss in ihrem Antrag auf die Registrierung der CVC-CA bei der gematik nachweisen, dass sie über die notwen­digen Qualifizierungen verfügt. Für die Ausstellung von CV-Rollen-Zertifikate mit einem Zugriffsprofil 0 oder 8 ist keine Qualifizierung erforderlich.

Für die Erzeugung von CV-Geräte-Zertifikaten benötigt die CVC-CA keine Quali­fizierung.

Grundsätzlich kann jedoch der Kartenherausgeber einen TSP-CVC seiner Wahl beauf­tragen. Zugelassene Produkttypen TSP-CVC bieten, abgesehen von der ggf. spezi­fischen Qualifizierung, die gleichen Funktionen (vgl. [gemKPT\_Arch\_TIP#5.2]).

### Kartenpersonalisierer

Der Begriff des Kartenpersonalisierers wird in [gemGlossar] definiert.

Der Kartenpersonalisierer kann bei der Produktion einer Chipkarte Dienstleistungen anderer Organisationen in Anspruch nehmen. Typische Dienstleistungen sind die Durchführung der Karteninitialisierung oder der Versand der produzierten Karten (Lettershop). Die genannten Dienstleistungen können aber auch durch den Kartenpersonalisierer selber vorgenommen werden. Ein konkretes Modell wird durch diese Spezifikation nicht vorgegeben.

### Zertifikatsnehmer

#### Karteninhaber (eGK)

Eine eGK enthält nur ein CV-Rollen-Zertifikat mit dem Zugriffsprofil 0. Durch eine C2C-Authen­tisierung mit einem HBA bzw. einer SMC erhalten die eGK und damit ihr Karteninhaber keine weiteren Zugriffsrechte auf Daten des HBA bzw. der SMC.

Im Rahmen der PKI für CV-Zertifikate hat daher ein Karteninhaber einer eGK keine besonderen zusätzlichen Zuständigkeiten bzw. Verpflichtungen.

#### Karteninhaber (HBA, SM-B für medizinische Institutionen oder Kostenträger)

Ein HBA bzw. eine SM-B für medizinische Institutionen oder Kostenträger enthält ein CV-Rollenzertifikat mit einem Zugriffsprofil ungleich 0. Das genaue Zugriffsprofil ist dabei abhängig von der Berufsgruppe, zu der der Karten­inhaber des HBA (Leistungserbringer, wie Arzt, Apotheker etc.) bzw. der SM-B gehört. Durch eine C2C-Authentisierung mit einer eGK erhält der HBA und damit sein Kartenin­haber weitere, von dem genauen Zugriffsprofil abhängige Zugriffsrechte auf die Daten der eGK.

Die Meldepflicht des Karteninhabers bei Verlust der Karte oder bei Änderung der Zugehörigkeit zu einer Berufsgruppe ist durch die übergreifende Anforderung [gemSpec\_PKI#GS-A\_4962] abgedeckt.

Konkrete Festlegungen hierzu werden durch die für die Ausgabe des HBA bzw. SMC-B zuständige Standesorganisation der Leistungserbringer geregelt.

Ein HBA oder eine SM-B für medizinische Institutionen oder Kostenträger enthaltenzusätzlich zu den CV-Rollenzertifikaten auch je ein CV-Gerätezertifikat. Aus dessen Existenz ergeben sich keine weiteren Pflichten für den Karteninhaber.

#### Karteninhaber (gSMC, SM-B für Gesellschafterorganisationen)

Eine gSMC oder ein SM-B für Gesellschafterorganisationen enthält keine CV-Rollenzertifikate. Durch eine C2C-Authentisierung mit einer anderen Chipkarte erhält die gSMC oder ein SM-B für Gesellschafterorganisationen und damit der Karteninhaber keine weiteren Zugriffsrechte auf in der anderen Chipkarte gespeicherte Daten.

Ein SM-B für Gesellschafterorganisationen ist im Gegensatz zu anderen SM-Bs nicht zum Zugriff auf eGKs berechtigt. Aus diesem Grund wird es nicht mit CV-Rollenzertifikaten ausgestattet und enthält nur ein CV-Gerätezertifikat.

## Nachbarsysteme

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

Die Beziehungen zu den Nachbarsystemen werden im Folgenden am Beispiel eines TSP-CVC eGK verdeutlicht.





Abbildung 1: Nachbarsysteme eines TSP-CVC eGK

Die Qualifizierung eines TSP-CVC zur Ausgabe von Rollenzertifikaten für den Zugriff auf medizinische Daten wird durch eine Standesorganisation der Leistungs­erbringer vergeben (Schritte 1 und 2). Die Festlegung von Anforderungen an eine Qualifi­zierung bzw. an die Durchführung des hierzu erforderlichen Prozesses ist nicht Gegen­stand des vorliegenden Dokuments. Für die Ausgabe von CV-Gerätezertifikaten ist keine Qualifizierung notwendig, ebenso wenig für die Erstellung von CV-Rollen-Zertifikaten mit dem Zugriffsprofil 0 (eGK) oder 8 (SM-B ohne Zugriff auf medizinische Daten).

Für den Prozess der Zulassung und Registrierung (Schritte 3 und 4) bestehen organisa­torische Schnittstellen zur gematik (s. Abschnitte 4.3 und 4.4). Der TSP-CVC beantragt bei der gematik die Zulassung des TSP-CVC und die Registrierung seiner CVC-CAs. Die gematik informiert den TSP-CVC über das Ergebnis des Zulassungsprozesses.

Für die Erzeugung der CV-Zertifikate des TSP-CVC bestehen technische und organisa­torische Schnittstellen zur CVC-Root-CA (Schritte 5 und 6) bzw. zum Anbieter der CVC-Root-CA (s. Abschnitt 3.1.1).

Die Erstellung und Ausgabe von CV-Zertifikaten (Schritt 7) für eGK, HBA, SM-B und gSMC erfolgt im Auftrag der jeweils verantwortlichen Kartenherausgeber (s. Abschnitt 3.1.2).

Der Kartenherausgeber kann die technischen Aufgaben und damit verbundenen organisatorischen Abläufe der Personalisierung der Karten durch den Kartenpersonalisierer an einen von ihm benannten Dritten übertragen (Schritt 8).

## Zugriffsprofile

Jedes CV-Zertifikat einer Chipkarte (eGK, HBA, SM-B, gSMC) enthält ein Zugriffsprofil.

Bei einem HBA und einer SM-B wird vorausgesetzt, dass sowohl das CV-Rollen-Zertifikat als auch die CV-Geräte-Zertifikate von der gleichen CVC-CA erzeugt wurden (vgl. gemKPT\_PKI\_TIP# 5.2).

Die Beschreibung von Zugriffsprofilen und deren normative Festlegung sind in [gemSpec\_PKI#6.3] und [gemSpec\_PKI#6.7.2.5] enthalten.

Mit seiner Zulassung erhält ein TSP-CVC das grundsätzliche Recht, CV-Zertifikate zu er­zeugen. Mit einer erfolgreichen Registrierung einer CVC-CA ist das Recht verbunden, CV-Zertifikate mit den bei der Registrierung zugeordneten Profilen zu generieren. Die Zulassung und Registrierung erfolgt durch die gematik.

Für spezifische Zugriffsprofile (z. B. das Rollenprofil 1) ist nicht nur eine Registrierung einer CVC-CA sondern auch eine Qualifizierung erforderlich. Die Zulassung und Regis­trierung erfolgt durch die gematik, eine Qualifizierung wird durch eine Standesorganisation der Leistungserbringer ausgesprochen. Die Bezeichnung „spezifische Zugriffsprofile“ wird im Folgenden verwendet, sofern die Ausgabe von CV-Zertifikaten mit solchen Zugriffsprofilen einer Qualifizierung bedarf. Dies sind insbesondere Zugriffsprofile ungleich 0 und 8.

Unabhängig von der technischen Umsetzung in CV-Zertifikaten werden in diesem Do­kument die Rollen gemäß der Bezeichnung für die Kartengeneration 1 verwendet (z.B. Rolle 1 für CV-Rollen-Zertifikat oder Rolle 51 für ein G2-CV-Geräte-Zerti­fikat). Die Umsetzung für die Kartengeneration 2 erfolgt dann gemäß den Vorgaben zum Parameter Certificate Holder Autorisation Template (CHAT) in [gemSpec\_PKI#6.7.2.5].

## Sperren und Nachladen von CV-Zertifikaten der Karten- generation 2

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

# 

# Übergreifende Festlegungen

## Erstellung Ausgabepolicy durch TSP-CVC

Gemäß [gemKPT\_PKI\_TIP#5.3] muss ein TSP-CVC für die Produktion von CV-Zertifi­katen eine Ausgabepolicy erstellen, die nicht im Widerspruch zu den übergeord­neten Ausgabepolicies stehen darf.

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

**⌦ TIP1-A\_2557 Inhalt der Ausgabepolicy des TSP-CVC**

Der TSP-CVC MUSS eine Ausgabepolicy erstellen, die mindestens die folgenden Punkte enthält:   
(a) Identifizierung von Anforderungen an den Betrieb,   
(b) Angaben zu organisatorischen und technischen Sicherheitsanforderungen,   
(c) Identifizierung von Antragstellern, die CV-Zertifikate beziehen möchten,   
(d) Festlegungen von Na­mens­regelungen zur CVC-CA,   
(e) Identifizierung von Profilen, für die CV-Zertifi­kate ausgestellt werden,   
(f) Angaben zu Zertifikatsprofilen,   
(g) Wirtschaftliche und Recht­liche Angelegenheiten sowie Angaben zur Haftung.

**⌫**

## Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-CVC

Gemäß [gemKPT\_PKI\_TIP#5.3] muss ein TSP-CVC für den Betrieb einer CVC-CA in einem Sicherheitskonzept den Gesamtprozess von der Beantragung bis zur Einbringung des CV-Zertifikates in eine Chipkarte beschreiben und die Einhaltung der beschriebenen Maß­nahmen auf Verlangen der TI-Plattform nachweisen. Sind mehrere Organisationen an diesem Prozess beteiligt, sind die technischen- und organisatorischen Schnittstellen 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#B].

**⌦ TIP1-A\_2558 Inhalt des Sicherheitskonzepts des TSP-CVC**

Der TSP-CVC MUSS ein Sicherheitskonzept gemäß den Vorgaben aus [gemSpec\_SiBetrUmg#B] erstellen.

**⌫**

**⌦ TIP1-A\_2592 Darstellung der Zusammenarbeit der beteiligten Akteure im Sicherheitskonzept**

In dem Sicherheitskonzept des TSP-CVC MUSS der TSP-CVC beschreiben, wie die technischen und organisatorischen Schnittstellen zwischen allen beteiligten Akteuren realisiert sind und wie die entsprechenden Sicherheitsmaßnahmen greifen.

**⌫**

Anforderungen an die Zusammenarbeit zwischen Kartenherausgeber, Kartenpersonalisierer und CVC-CA sind auch Gegenstand von Abschnitt 4.5.

## Zulassung

Ein TSP-CVC benötigt eine aktuelle Zulassung bei der gematik, um ein CV-Zertifikat für seine CVC-CA bei der CVC-Root-CA zu beantragen.

Eine CVC-CA der zweiten Ebene können verschiedene Organisationen betreiben. Beispiele sind:

* Kartenherausgeber,
* Kartenpersonalisierer,
* TSP-X.509.

## Registrierung und Qualifizierung

Damit der TSP-CVC CV-Zertifikate für Karten eines Kartenherausgebers ausstellen kann, muss hierfür eine Registrierung durch die gematik vorgenommen werden. Mit der Regis­trierung wird festgelegt, für welche(s) Profil(e) CV-Zertifikate mit dieser CVC-CA generiert werden können.

Die Darstellung des Registrierungsprozesses ist Gegenstand der Verfahrensbeschreibung zur Registrierung einer CVC-CA.

**⌦ TIP1-A\_2564 Erzeugen von CV-Zertifikaten mit registrierten Zugriffsprofilen**

Eine CVC-CA MUSS sicherstellen und nachweisen, dass sie nur CV-Zertifikate mit Zugriffsprofilen erzeugt, die bei ihrer Registrierung festgelegt wurden.

**⌫**

**⌦ TIP1-A\_2565 Einholung von Qualifizierungen**

Für spezifische Profile MUSS der TSP-CVC zur Erzeugung von CV-Zertifikaten eine Autorisierung durch eine Standesorganisation der Leistungserbringer einholen (Qualifizierung).

**⌫**

**⌦ TIP1-A\_2690 Ausstellen von Qualifizierungen**

Für spezifische Profile MÜSSEN Standesorganisationen der Leistungserbringer unter den Voraussetzungen von [TIP1-A\_2567] den TSP-CVC zur Ausgabe von CV-Zertifikaten autorisieren.

**⌫**

Mit dem im CV-Zertifikat enthaltenen Profil sind Zugriffsrechte auf Daten der Versicherten in der eGK verbunden. Diese Rechte müssen den Vorgaben des § 291a SGB V ent­sprechen. Die Bedingungen hierfür legen die zuständigen Organisationen fest. Falls eine CVC-CA CV-Zertifikate für einen HBA bzw. eine SM-B mit Rollen-Profil ungleich 8 erzeugt, benötigt sie hierfür eine entsprechende Qualifizierung durch die für die Heraus­gabe dieser Karten zuständige Standesorganisation der Leistungserbringer.

**⌦ TIP1-A\_2566 Nachweis über die Qualifizierung**

Sofern die CVC-CA CV-Zertifikate mit spezifischen Profilen ausgibt, MUSS die CVC-CA im Rahmen des Zulassungs- und Registrierungsprozesses einen Nach­weis über die Qualifizierung, die die CVC-CA zur Ausgabe von CV-Zertifikaten mit spezifischen Profilen berechtigt, erbringen.

**⌫**

**⌦ TIP1-A\_2567 Spezifische Anforderungen an den TSP-CVC im Kontext einer Qualifizierung**

Eine Standesorganisation der Leistungserbringer KANN an eine CVC-CA für die Aus­gabe von CV-Zertifikaten mit bestimmten Zugriffsprofilen zusätzlich eigene An­for­derungen stellen, die über die in diesem Dokument genannten Mindestanfor­de­rungen der gematik hinausgehen.

**⌫**

Die Beschreibung zusätzlicher Anforderungen einer Standesorganisation der Leistungs­erbringer sowie Festlegungen zum Prozess der Qualifizierung einer CVC-CA liegen in der Verantwortung der jeweiligen Organisation. Mit einem Formular bestätigt die Organisation gegenüber der gematik, dass die Qualifizierung für die CVC-CA erfolgreich durchgeführt wurde. Im Rahmen der Registrierung überprüft die gematik das Vorhandensein der Quali­fizierung und dass der Nachweis durch eine berechtigte Person unterzeichnet wurde. Inhaltliche Überprüfungen der Qualifizierung werden durch die gematik nicht durchgeführt. Im Vorfeld teilen die zuständigen Standesorganisationen der Leistungserbringer der gematik mit, welche ihrer Mitarbeiter zeichnungsberechtigt für die Nachweise sind.

**⌦ TIP1-A\_2568 Erzeugen von CV-Zertifikaten mit Profilen, die einer Qualifi­zierung bedürfen**

Eine CVC-CA MUSS sicherstellen, dass CV-Rollen-Zertifikate für einen HBA bzw. ein Sicherheitsmodul vom Typ B (nur Sicherheitsmodule mit vorgesehenem Rollen-Profil ungleich 8) nur mit solchen Zugriffsprofilen erzeugt werden, für die im Rahmen des Zulassungsprozesses die notwendigen Berechtigungsnachweise der zustän­digen Standesorganisationen der Leistungserbringer vorgelegen haben. Ab­weichun­gen hiervon führen zu einem unverzüglichen Widerruf der Registrierung.

**⌫**

Eine Zuordnung welche Standesorganisation der Leistungserbringer verantwortlich für die jeweilige Qualifizierung ist, ist in [gemSpec\_PKI#6.3.1] festgelegt.

## Zusammenspiel Kartenherausgeber, CVC-CA und Kartenpersonalisierer

Bei dem Prozess der Ausgabe einer personalisierten Chipkarte (eGK, HBA, SM-B, gSMC) müssen Kartenherausgeber, Kartenpersonalisierer, CVC-CA und CAs anderer PKI zusammenarbeiten (sofern der Kartenherausgeber diese Funktionen nicht selbst ausführt). Die genaue Aufgabenteilung wird nicht einheitlich vorgegeben. Bei der Produktion ver­schie­dener Karten sind unterschiedliche Formen der Zusammenarbeit und der Aufgaben­teilung denkbar. Dabei obliegt die technische Durchführung der in den folgenden Anforderungen enthaltenen Aufgaben i.d.R. dem Kartenpersonalisierer. Der Kartenherausgeber ist jedoch gesamtverantwortlich für die Ausgabe der Karte.

Für die Sicherheit der PKI für CV-Zertifikate müssen die folgenden Ziele erreicht bzw. die folgenden Anforderungen erfüllt werden.

**⌦ TIP1-A\_2575 Zugelassenes Zugriffsprofil im CV-Rollen-Zertifikat**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS sicherstellen, dass in dem CV-Rollen-Zertifikat einer Chipkarte ein für den Karteninhaber der Chipkarte zugelassenes Zugriffsprofil (Feld CHA bei Kartengeneration 1 und Feld CHAT bei Kartengeneration 2) kodiert wird.

**⌫**

*Hinweis: Eine gSMC enthält kein CV-Rollen-Zertifikat.*

**⌦ TIP1-A\_2576 Zugelassenes Zugriffsprofil im CV-Geräte-Zertifikat**

Der Kartenpersonalisierer HBA,SM-B oder gSMC MUSS sicherstellen, dass in einem CV-Geräte-Zertifikat einer Chipkarte ein bestimmtes Zugriffsprofil genau dann kodiert wird, falls das Gerät die entsprechende Funktionseinheit unterstützt.

**⌫**

*Hinweis: Eine eGK enthält als eigenes CV-Zertifikat nur ein CV-Rollen-Zertifikat (C.eGK.AUT\_CVC).*

**⌦ TIP1-A\_2578 Korrekte ICCSN der Chipkarte**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS sicherstellen, dass in dem CV-Zertifikat einer Chipkarte die korrekte ICCSN der Chipkarte (Feld CHR) kodiert wird.

**⌫**

**⌦ TIP1-A\_2579 Korrekter privater Schlüssel in der Chipkarte**

Der Kartenpersonalisierer MUSS sicherstellen, dass nach Produktion und Personalisierung der Chipkarte der private Schlüssel enthalten ist, der zu dem durch das enthaltene CV-Zertifikat zertifizierten öffentlichen Schlüssel gehört.

**⌫**

**⌦ TIP1-A\_2580 Erzeugung des privaten Schlüssels der Chipkarte**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS die Sicherheit des privaten Schlüssels bei dessen Erzeugung gewährleisten. Das bedeutet, dass der private Schlüssel in einem HSM bzw. einer Chipkarte generiert wird.

**⌫**

**⌦ TIP1-A\_2581 Evaluierung von HSMs**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS beim Einsatz eines HSM bzw. einer Chipkarte sicherstellen, dass deren 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.

**⌫**

**⌦ TIP1-A\_2582 Vertraulichkeit des privaten Schlüssels der Chipkarte**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS die Vertraulichkeit des privaten Schlüssels gewährleisten und sicherstellen, dass der private Schlüssel außerhalb des HSM nicht im Klartext vorhanden ist und nach der Personalisierung in die Chipkarte in allen anderen HSM gelöscht wird.

**⌫**

**⌦ TIP1-A\_2583 Zuordnung des privaten Schlüssels zu Identitäten**

Der Kartenherausgeber oder ein von ihm benannter Dritter Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS sicherstellen, dass ein privater Schlüssel nicht zwei verschiedenen Identitäten zugeordnet wird.

**⌫**

**⌦ TIP1-A\_2584 Schlüsselpaare und CV-Zertifikate**

Benötigt eine Chipkarte mehrere CV-Zertifikate, da sie mit verschiedenen Zugriffs­profilen C2C-Authentisierungen durchführen muss (z. B. ein HBA), MUSS der Kartenpersonalisierer sicherstellen, dass für jedes CV-Zertifikat ein eigenes Schlüsselpaar verwendet wird.

**⌫**

*Hinweis: Eine eGK enthält als eigenes CV-Zertifikat nur ein CV-Rollen-Zertifikat (C.eGK.AUT\_CVC) mit dem Zugriffsprofil 0.   
Eine gSMC-KT enthält als eigenes CV-Zertifikat nur ein CV-Geräte-Zertifikat (C.SMC.AUTD\_RPS\_CVC) mit dem Zugriffsprofil 54.*

**⌦ TIP1-A\_2585 Personalisierung von CV-Zertifikaten für einen HBA**

Bei der Personalisierung eines HBA MUSS der Kartenpersonalisierer sicherstellen, dass die einzubringenden CV-Zertifikate entweder genau das Zugriffsprofil enthalten, das zu der Rolle der Leistungserbringergruppe (z. B. Arzt, Apotheker, etc.) gehört, für die der HBA produziert wird, oder das Zugriffsprofil, das zu einer Funktionseinheit gehört, die (als Kartenanwendung) in einem HBA enthalten ist.

**⌫**

**⌦ TIP1-A\_2586 Personalisierung von CV-Zertifikaten für ein Sicherheitsmodul vom Typ B**

Bei der Personalisierung eines Sicherheitsmoduls vom Typ B MUSS der Kartenpersonalisierer sicherstellen, dass die einzubringenden CV-Zertifikate entweder genau das Zugriffsprofil enthalten, das zu der Rolle der entsprechenden Einrichtung gehört, für die das Sicherheitsmodul produziert wird, oder das Zugriffsprofil, das zu einer Funktionseinheit gehört, die (als Kartenan­wendung) im Sicherheitsmodul enthalten ist.

**⌫**

**⌦ TIP1-A\_2587 Personalisierung von CV-Zertifikaten für eine eGK**

Bei der Personalisierung einer eGK MUSS der Herausgabeverantwortliche gemäß Kapitel 1.6 sicherstellen, dass das einzubringende CV-Zertifikat genau das Zugriffs­profil 0 enthält.

**⌫**

Der Schutzbedarf bezüglich des Schutzziels „Authentizität“ des öffentlichen Schlüssels der CVC-Root-CA ist „sehr hoch“.

**⌦ TIP1-A\_4222 Authentizität des öffentlichen Root-Schlüssels**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS vor der Verwendung des öffentlichen Schlüssels der CVC-Root-CA die Authentizität dieses Schlüssels sicherstellen.

Bei der Personalisierung einer Chipkarte MUSS der Herausgabeverantwortliche gemäß Kapitel 1.6 sicherstellen, dass der korrekte aktuelle öffentliche Schlüssel der CVC-Root-CA eingebracht wird.   
Dabei MUSS der Kartenherausgeber oder ein von ihm benannter Dritter durchgängig das Vier-Augen-Prinzip umsetzen.   
Die Umsetzung MUSS zwingend in einem entsprechenden Organi­sations­kon­zept als Teil des Sicherheitskonzepts beschrieben sein.

**⌫**

**⌦ TIP1-A\_2589 Personalisierung des CVC-CA-Zertifikats**

Bei der Personalisierung einer Chipkarte MUSS der Herausgabeverantwortliche gemäß Kapitel 1.6 sicherstellen, dass das korrekte CVC-CA-Zertifikat der CVC-CA eingebracht wird, die das enthaltene CV-Zertifikat erzeugt hat.

**⌫**

**⌦ TIP1-A\_2590 Vernichtung fehlerhafter Chipkarten vor deren Ausgabe**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS Chipkarten, die vor Ausgabe an den Karteninhaber als fehlerhaft erkannt werden, ordnungsgemäß vernichten.

**⌫**

**⌦ TIP1-A\_2591 Ausgabe fehlerfreier Chipkarten**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS Chipkarten, die fehlerfrei produziert und personalisiert wurden, an den vorgesehenen Karteninhaber übergeben oder diese vernichten, falls sie nicht übergeben werden können.

**⌫**

Die genannten Anforderungen können nicht nur durch Sicherheitsmaßnahmen bei einem der an der Produktion beteiligten Organisationen erreicht werden. Es ist vielmehr eine zwischen den Beteiligten abgestimmte Zusammenarbeit verschiedener Sicherheits­maßnah­men der beteiligten Organisationen notwendig. Diese Zusammenarbeit ist im Sicherheitskonzept darzustellen (s. Abschnitt 4.2).

## Mindestanforderungen an eine CVC-CA

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

### Schutzbedarfsfeststellung

**⌦ TIP1-A\_2593 Schützenswerte Objekte des TSP-CVC**

Die folgenden sicherheitsrelevanten bzw. sensitiven Objekte MÜSSEN durch den TSP-CVC als schützenswerte Objekte im Sicherheitskonzept des TSP-CVC berück­sich­tigt werden:   
(a) Privater Schlüssel der CVC-CA,   
(b) Öffentlicher Schlüssel der CVC-CA,   
(c) Öffentlicher Schlüssel der CVC-Root-CA,   
(d) Öffentlicher Schlüssel einer eGK zur Rollenauthentisierung,   
(e) Öffentlicher Schlüssel eines HBA bzw. eines Sicherheitsmoduls vom Typ B zur Rollenauthentisierung,   
(f) Öffentlicher Schlüs­sel eines HBA, eines Sicherheitsmoduls vom Typ B bzw. einer geräte­bezogenen SMC zur Authentisierung mit Geräte-Profilen,   
(g) Zertifikatsantrag für CVC-CA-Zertifikat,   
(h) Zertifikatsantrag für ein CV-Zertifikat einer Chipkarte,   
(i) Zulassungsdokumente,   
(j) Registrierungsdokumente,   
(k) Qualifizierungsdokumente,   
(l) Authentisierungsinformationen zur Authentisierung von Akteuren bzw. Rollen,  
(m) Protokolldaten und   
(n) Konfigurationsdaten.

**⌫**

**⌦ TIP1-A\_2594 Vorgaben zum Schutzbedarf durch die gematik**

Der TSP-CVC MUSS die Vorgaben der gematik hinsichtlich der Einstufung des Schutz­bedarfs gemäß dem Ergebnis der Schutzbedarfsfeststellung der TI berück­sichtigen. Weiterhin MUSS er für die Definition spezifischer Einstufungen die Vorgaben für die Methode zur Schutzbedarfsfeststellung in der TI anwenden.

**⌫**

**⌦ TIP1-A\_2595 Spezifische Erhöhung des Schutzbedarfs ist zulässig**

Die Einstufung des Schutzbedarfs KANN durch den TSP-CVC spezifisch erhöht werden.

**⌫**

**⌦ TIP1-A\_2596 Schutzbedarf darf nicht erniedrigt werden**

Eine niedrigere Einstufung des Schutzbedarfs DARF durch den TSP-CVC NICHT vorgenommen werden.

**⌫**

### Verfügbarkeit der CVC-CA

Anforderungen für die Verfügbarkeit der CVC-CA werden nicht vorgegeben.

### Ausschließlichkeit und Dauer der Schlüsselnutzung

**⌦ TIP1-A\_2598 Verwendung des Schlüsselpaars der CVC-CA**

Der TSP-CVC MUSS sicherstellen, dass das Schlüsselpaar einer CVC-CA, für das durch die CVC-Root-CA ein CVC-CA-Zertifikat erstellt wurde, ausschließlich für das Erstellen von CV-Zertifikaten der für diese CVC-CA registrierten Profile eingesetzt wird.

**⌫**

**⌦ TIP1-A\_2599 Begrenzung der Lebensdauer des Schlüsselpaars der CVC-CA**

Der TSP-CVC MUSS die Lebensdauer des Schlüsselpaares der CVC-CA begren­zen. Er MUSS das Schlüsselmanagement der CVC-CA in seinem Sicher­heits­konzept beschreiben und umsetzen.

**⌫**

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

**⌦ TIP1-A\_2600 Gültigkeitsdauer der CVC-CA Schlüssel**

Der TSP-CVC MUSS sicherstellen, dass die Lebensdauer des Schlüsselpaars der CVC-CA eine Gültigkeitsdauer von 8 Jahren nicht überschreitet.

**⌫**

**⌦ TIP1-A\_2601 Ablauf der Gültigkeitsdauer des privaten Schlüssels der CVC-CA**

Mit Ablauf der Gültigkeitsdauer DARF der private Schlüssel der CVC-CA durch den TSP-CVC NICHT mehr für das Erstellen von Signaturen von CV-Zertifikaten eingesetzt werden.

**⌫**

Für diese CVC-CA ist dann eine erneute Registrierung erforderlich.

**⌦ TIP1-A\_2602 Weiterverwendung des privaten Schlüssels einer CVC-CA**

Ein TSP-CVC DARF den privaten Schlüssel einer CVC-CA NICHT weiterhin verwenden, falls für die CVC-CA ein neues Schlüsselpaar generiert wurde oder falls die Zulassung des TSP-CVC durch die gematik widerrufen wurde.

**⌫**

**⌦ TIP1-A\_2603 Vernichtung nicht mehr benötigter Schlüssel**

Der TSP-CVC MUSS sicherstellen, dass nicht mehr benötigte Schlüssel einer CVC-CA sicher gelöscht werden. Dies MUSS im Sicherheitskonzept des TSP-CVC dargestellt werden.

**⌫**

Zur sicheren Löschung von Schlüsseln können die Maßnahmen gemäß Abschnitt 4.6.4 verwendet werden.

### Verlust der Zulassung

**⌦ TIP1-A\_2604 Vernichtung der privaten Schlüssel bei Verlust der Zulassung**

Falls der TSP-CVC seine Zulassung bei der gematik verliert, MUSS er alle privaten Schlüssel, für die er ein CVC-CA-Zertifikat der CVC-Root-CA besitzt, nach expliziter Anordnung der gematik vernichten.

**⌫**

**⌦ TIP1-A\_2605 Maßnahmen zur Vernichtung von Schlüsseln**

Der TSP-CVC 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\_2606 Information über die Vernichtung aller Schlüsselpaare an gematik**

Der TSP-CVC 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\_2607 Einsatz eines HSM**

Der TSP-CVC MUSS für die Sicherheit des Schlüsselpaares einer CVC-CA ein HSM einsetzen.

**⌫**

**⌦ TIP1-A\_2608 Speicherung und Anwendung des privaten Schlüssels in einem HSM**

Der TSP-CVC MUSS sicherstellen, dass   
a) der private Schlüssel für die Erzeugung von Zertifikaten nicht auslesbar in einem Hardware-Sicherheitsmodul (HSM) ge­speichert wird 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\_2609 Einsatz einer Chipkarte als HSM**

Bei einem TSP-CVC KANN als HSM auch eine Chipkarte zum Einsatz kommen.

**⌫**

**⌦ TIP1-A\_4223 Ordnungsgemäße Sicherung des privaten Schlüssels der CVC-CA**

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

**⌫**

**⌦ TIP1-A\_4224 Verwendung von privaten Schlüsseln einer CVC-CA**

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

**⌫**

**⌦ TIP1-A\_2610 Möglichkeit zum Klonen eines HSM**

Falls notwendig KANN aus Gründen der Hochverfügbarkeit bzw. hoher Perfor­manz­anforderungen (Möglichkeit zur Lastverteilung) durch den TSP-CVC ein HSM "geklont" werden, indem der private Schlüssel aus dem HSM (kryptographisch abgesichert) exportiert wird und in ein weiteres HSM importiert wird.

**⌫**

Für das Klonen eines HSMs müssen die folgenden Anforderungen berücksichtigt werden:

**⌦ TIP1-A\_2611 Berücksichtigung des Klonens im Sicherheitskonzept**

Der TSP-CVC MUSS den Vorgang des Klonens (ggf. auch abgebildet über Schlüsselbackup und -restore) im Sicherheitskonzept gesondert beschreiben.   
Dabei MÜSSEN insbesondere die Maßnahmen für die Gewährleistung der Sicherheit des privaten Schlüssels als auch die (technischen und/oder organisatorischen) Maßnahmen für die Verhinderung des unautorisierten Erstellens von Klonen beschrieben werden.

**⌫**

**⌦ TIP1-A\_2612 Anwendung des Vier-Augen-Prinzips beim Klonen eines HSMs**

Der TSP-CVC MUSS sicherstellen, dass der Prozess zum Klonen eines HSM nur durch zwei Mitarbeiter (Vier-Augen-Prinzip), die sich erfolgreich authentisiert haben, ausgeführt werden kann.

**⌫**

**⌦ TIP1-A\_2613 Protokollierung beim Klonen eines HSMs**

Das Klonen eines HSM MUSS durch den TSP-CVC protokolliert werden.

**⌫**

**⌦ TIP1-A\_2614 Nachvollziehbarkeit über die Klone eines HSMs**

Durch den TSP-CVC MUSS zu jeder Zeit einfach nachvollziehbar sein, wie viele Klone des HSM existieren.

**⌫**

Alle Klone eines HSM (d. h. alle HSM mit dem gleichen privaten Schlüssel) werden im Sinne dieses Dokuments logisch als ein HSM betrachtet, d.h. alle Anforderungen an ein HSM gelten für jeden Klon.

**⌦ TIP1-A\_2615 Einsatz der Klone eines HSMs im geschützten Bereich der Betriebsstätte**

Alle Klone eines HSM (d. h. alle HSM mit dem gleichen privaten Schlüssel) MÜSSEN durch den TSP-CVC in einem geschützten Bereich der Betriebsstätte ein­ge­setzt werden.

**⌫**

**⌦ TIP1-A\_2616 Evaluierung von HSMs – TSP-CVC**

Als HSM MUSS der TSP-CVC ein Modul (bzw. eine Chipkarte) 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\_2617 Vorgaben an die Funktionalität des HSM der CVC-CA**

Der TSP-CVC 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\_4225 Nutzung eines HSM nach erfolgreicher Benutzerauthentisierung**

Der TSP-CVC MUSS sicherstellen, dass das HSM nur nach einer erfolgreichen Benutzerauthentisierung genutzt werden kann.

**⌫**

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

**⌦ TIP1-A\_5381 Zugang zu HSM-Systemen im Vier-Augen-Prinzip**

Der TSP-CVC 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\_2618 Weitergabe sensitiver Schlüssel**

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

**⌫**

**⌦ TIP1-A\_2619 Authentizität des öffentlichen Schlüssels der CVC-CA bei Zertifikatsbeantragung**

Bei der Beantragung und Generierung eines Zertifikats für die CVC-CA MUSS durch den TSP-CVC die Authentizität des öffentlichen Schlüssels sichergestellt werden. Da­zu MUSS ein Fingerprint über den öffentlichen Schlüssel in dem Antrags­schrei­ben an die CVC-Root-CA übermittelt werden und ein mit dem privaten Schlüssel sig­nierter (den öffentlichen Schlüssel enthaltenen) Request an die CVC-Root-CA übermittelt werden.

**⌫**

Die genauen Formate für den Fingerprint und den CVC-PKCS#10-Request (vgl. Abschnitt 4.7) werden durch den Anbieter der CVC-Root-CA vorgegeben.

**⌦ TIP1-A\_2620 Backup und Verfügbarkeit der CVC-CA für Produktiv- und Testumgebung**

Der TSP-CVC MUSS   
a) für die Verfügbarkeit der CVC-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 CVC-CA nach den vom HSM-Hersteller vorgegebenen Backup-Verfahren sicher erstellen und sicher verwahren,   
c) im Falle einer notwendigen Löschung des privaten Schlüssels auch das zugehörige Schlüsselbackup auf sichere Weise löschen.

**⌫**

**⌦ TIP1-A\_2621 Backup-HSMs – sicherer Schlüsseltransport CVC-CA**

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

**⌫**

**⌦ TIP1-A\_2622 Erzeugung eines Backup-HSMs – Einhaltung weiterer Vorgaben**

Bei dem Erzeugen des Backup-HSMs MÜSSEN durch den TSP-CVC die definierten Vorgaben für das Klonen von HSMs sowie die Vorgaben an die Umsetzung des Vier-Augen-Prinzips eingehalten werden.

**⌫**

### Algorithmen und Schlüssellängen

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

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

### Schlüsselversionen

CVC-CAs der zweiten Ebene setzen für das Ausstellen von CV-Zertifikaten ein Schlüs­sel­paar ein, dass eine gegebene feste 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-CAs der zweiten Ebene 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 eine 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.

**⌦ TIP1-A\_2626 Berücksichtigung von Notfallmaßnahmen im Sicherheitskonzept**

Eine Abschätzung der Auswirkungen einer Kompromittierung eines Schlüsselpaares sowie die daraus folgenden Notfallprozesse MÜSSEN durch den TSP-CVC in einer Risikoanalyse und Notfallplanung in seinem Sicherheitskonzept behandelt werden.

**⌫**

Kommt es bei einer CA der zweiten Ebene zu einem Versionswechsel bei dem Schlüssel­paar für das Ausstellen von CV-Zertifikaten, kann dieser Fall logisch behandelt werden, wie das Aufsetzen einer neuen CA.

**⌦ TIP1-A\_2627 Wechsel der Schlüsselversion bei der CVC-CA**

Im Falle eines Wechsels der Schlüsselversion MUSS der TSP-CVC den neuen öffentlichen Schlüssel einer CVC-CA durch die CVC-Root-CA zertifizieren lassen. Bei allen im Folgenden durch die CVC-CA zu erzeugenden CV-Zertifikate MUSS die CVC-CA ihr neues Schlüsselpaar verwenden. Entsprechend MUSS bei der Kartenproduktion das neue CV-Zertifikat der CVC-CA in die zugehörigen Karten eingebracht werden.

**⌫**

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.

### Protokollierung

**⌦ TIP1-A\_2628 Protokollierung durch den TSP-CVC - Ereignisse**

Die Arbeit des TSP-CVC MUSS revisionssicher protokolliert werden. Mindestens die folgenden Ereignisse MÜSSEN durch den TSP-CVC protokolliert werden:   
(a) Generierung eines neuen Schlüsselpaares im HSM,   
(b) Löschung eines privaten Schlüssels im HSM,   
(c) Export des privaten Schlüssels,   
(d) Import des privaten Schlüssels,   
(e) Sperrung der Zugriffe auf einen privaten Schlüssel im HSM,   
(f) Erzeugen eines CV-Zertifikats mit einem Profil ungleich 0 (CV-Zertifikat für einen HBA, ein Sicherheitsmodul vom Typ B oder ein gerätebezogenes Sicherheitsmodul),   
(g) Erzeugen einer Menge von CV-Zertifikaten mit Profil 0 (CV-Zertifikat für eine eGK).

**⌫**

**⌦ TIP1-A\_2691 Protokollierung durch den TSP-CVC - Werte**

Bei der Protokollierung MÜSSEN durch den TSP-CVC die folgenden Werte protokolliert werden:   
(a) Datum und Uhrzeit,   
(b) Typ des Ereignisses,   
(c) Namen der beiden Mitarbeiter des TSP-CVC, die das HSM frei geschaltet haben.

**⌫**

**⌦ TIP1-A\_2629 Protokollierung durch den TSP-CVC – Profil ungleich 0**

Bei dem Erzeugen eines CV-Zertifikates mit einem Profil ungleich 0 MÜSSEN durch den TSP-CVC zusätzlich die folgenden Werte protokolliert werden:   
(a) Name des zu­ständigen Kartenherausgebers,   
(b) Inhalt der Felder CHR und CHA bei Kar­ten­generation 1 und Inhalt der Felder CHR und CHAT bei Kartengeneration 2,   
(c) das erstellte CV-Zertifikat selber.

**⌫**

**⌦ TIP1-A\_2692 Protokollierung durch den TSP-CVC – Profil gleich 0**

Der TSP-CVC MUSS bei dem Erzeugen von CV-Zertifikaten mit einem Profil gleich 0 die folgenden Werte protokollieren:   
(a) Name des zuständigen Kartenherausgebers,   
(b) Inhalt der Felder CHR und CHA bei Kartengeneration 1 und Inhalt der Felder CHR und CHAT bei Kartengeneration 2,   
(c) das erstellte CV-Zertifikat selber,   
(d) Anzahl der erzeugten CV-Zertifikate.

**⌫**

**⌦ TIP1-A\_2630 Protokollierung pro Bestellung/Produktionslauf (Profil gleich 0)**

Die Protokollierung durch den TSP-CVC bei dem Erzeugen von CV-Zertifikaten mit Profil gleich 0 SOLL pro Bestellung/Produktionslauf geschehen.

**⌫**

**⌦ TIP1-A\_2631 Nachvollziehbarkeit bei Produktion mit Profil 0**

Der TSP-CVC MUSS sicherstellen, dass dabei nachträglich anhand der Protokolle nachvollzogen werden kann, wann wie viele CV-Zertifikate mit einem Profil gleich 0 für wen erzeugt wurden.

**⌫**

**⌦ TIP1-A\_2632 Schutz der Protokolldaten gegen Manipulation**

Der TSP-CVC 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\_2633 Prüfung der Protokolldaten durch die gematik**

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

**⌫**

### Personelle Anforderungen

**⌦ TIP1-A\_2634 Berücksichtigung von Rollen**

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

**⌫**

Mit "Leiter CVC-CA" wird der Leiter des TSP-CVC bezeichnet. Der "Sicherheitsbeauf­tragte CVC-CA" ist eine vom "Leiter CVC-CA" ernannte Person, die die Aufgabe Infor­mationssicherheit koordiniert und vorantreibt. Die Rolle "Zertifizierer" ist dabei für das Generieren von CV-Zertifikaten für eGKs, HBAs, SM-Bs bzw. gSMCs zuständig. Die Rolle "Antragsteller CVC-CA-Zertifikat" ist dagegen für das persönliche Überbringen des CVC-PKCS#10-Requests zur CVC-Root-CA zuständig. Der Datenschutzbeauftragte ist eine vom "Leiter CVC-CA" bestellte Person, die für den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten verantwortlich ist.

**⌦ TIP1-A\_2635 Definition der Rollen und Festlegungen ihrer Aufgaben**

Der TSP-CVC 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\_2636 Benennung von Mitarbeitern gegenüber gematik**

Der TSP-CVC MUSS der gematik die verantwortlichen Mitarbeiter für die Rollen "Leiter CVC-CA", "Sicherheitsbeauftragter CVC-CA" und "Antragsteller CVC-CA-Zertifikat" mitteilen. Für die Rolle "Leiter CVC-CA" MUSS dabei auch ein Stellver­treter genannt werden. Der TSP-CVC MUSS der gematik Änderungen an der Zuordnung von Rollen mitteilen.

**⌫**

**⌦ TIP1-A\_2637 Berücksichtigung von Zugriffen auf das HSM im Vier-Augen-Prinzip**

Der TSP-CVC MUSS sicherstellen, dass keine einzelne Person zwei Rollen ausüben kann, die Zugriffe auf das HSM im Vier-Augen-Prinzip für diese einzelne Person ermöglicht.

**⌫**

### Betriebliche Anforderungen

**⌦ TIP1-A\_2641 Geschützter Bereich**

Der TSP-CVC MUSS das HSM in einem geschützten Bereich der Betriebsstätte unterbringen. Für diesen Bereich der Betriebsstätte des TSP-CVC 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\_2642 Verwendung mehrerer geschützter Bereiche**

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

**⌫**

**⌦ TIP1-A\_2644 Schutz von HSM-Klonen**

Der TSP-CVC MUSS Maßnahmen beschreiben, ergreifen und nachweisen, die verhindern, dass ein HSM oder eines seiner Klone aus einem der geschützten Bereiche unautorisiert entfernt werden kann.

**⌫**

**⌦ TIP1-A\_2645 Zugriffe auf Systeme der CVC-CA über Arbeitsplatzrechner (oder Systeme) außerhalb des geschützten Bereichs**

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

**⌫**

**⌦ TIP1-A\_2647 Sicherer Betrieb von Systemkomponenten**

Der TSP-CVC 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.

**⌫**

### Authentizität des öffentlichen Schlüssels der CVC-CA

Der Anbieter der CVC-Root-CA setzt für den Prozess der Ausstellung eines Zertifikats durchgängig in und zwischen allen Arbeitsschritten, d.h. vom Eingang des Zertifikatsaus­stellungsantrags bis hin zur Übergabe des Zertifikats an den Antragssteller, das Vier-Augen-Prinzip um.

**⌦ TIP1-A\_2648 Vier-Augen-Prinzip bei Beantragung des CVC-CA-Zertifikats**

Der TSP-CVC MUSS für den Gesamtprozess der Beantragung und des Erhalts eines CVC-CA-Zertifikats bei einer CVC-Root-CA das Vier-Augen-Prinzip umsetzen.

**⌫**

Dies kann bspw. dadurch erfolgen, dass den Zertifikatsausstellungsantrag zwei Mitar­beiter der CVC-CA auf Korrektheit direkt vor der Abgabe an den Anbieter der CVC-Root-CA im Vier-Augen-Prinzip prüfen und diese Prüfung dokumentieren.

**⌦ TIP1-A\_2649 Konsistenzprüfung des ausgestellten CVC-CA-Zertifikats**

Bei erfolgreicher Ausstellung des beantragten Zertifikats MÜSSEN mindestens zwei Mitarbeiter des TSP-CVC das von der CVC-Root-CA übergebene Zertifikat auf Kon­sis­tenz bezüglich des Zertifikatsausstellungsantrags prüfen sowie das Prüfergebnis dokumentieren und revisionssicher aufbewahren.

**⌫**

**⌦ TIP1-A\_2650 Behandlung negativer Prüfergebnisse im Sicherheitskonzept**

Für fehlgeschlagene Prüfergebnisse MUSS der TSP-CVC Notfallmaßnahmen in seinem Sicherheitskonzept definieren und diese im Eintrittsfalle einleiten.

**⌫**

Das bei Ausstellung eines Zertifikats durch die CVC-Root-CA angewandte Vier-Augen-Prinzip muss mit dem Vier-Augen-Prinzip der Beantragung und des Erhalts des Zertifikats durch den TSP-CVC so ineinandergreifen, dass die Durchgängigkeit des Vier-Augen-Prinzip garantiert ist.

### Synchronisierung mit dem Zeitdienst

**⌦ TIP1-A\_2695 Verfahren zur Zeitsynchronisierung**

Ein TSP-CVC MUSS ein Verfahren zur Zeitsynchronisierung einsetzen, das eine maximale Abweichung von einer Sekunde gegenüber der gesetzlichen Zeit der Physikalisch-Technischen Bundesanstalt (PTB) gewährleistet.

**⌫**

## Beantragung eines CV-Zertifikats für die CVC-CA

Nach erfolgreicher Zulassung und Registrierung kann ein TSP-CVC für einen öffentlichen Schlüssel einer CVC-CA ein CVC-CA-Zertifikat bei der CVC-Root-CA beantragen. Die Fest­legungen zur Nutzung der organisatorischen Schnittstelle P\_Sub\_CA\_Certifi­cation\_CVC durch den TSP-CVC werden im Folgenden beschrieben.

Die Beantragung geschieht in zwei Schritten:

* Der TSP-CVC stellt einen schriftlichen Antrag bei der CVC-Root-CA. Als Antwort wird ihm ein Termin mitgeteilt, an dem der 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 an die CVC-Root-CA. Nach Bearbeitung erhält er das neue CVC-CA-Zertifikat.

**⌦ TIP1-A\_2654 Antrag für ein CVC-CA-Zertifikat bei der CVC-Root-CA**

Der TSP-CVC MUSS ein neues CVC-CA-Zertifikat für ihr Schlüsselpaar schriftlich bei der CVC-Root-CA beantragen. Hierzu MUSS der TSP-CVC die von der CVC-Root-CA zur Verfügung gestellte Schnittstelle P\_Sub\_CA\_Certification\_CVC nutzen.

**⌫**

**⌦ TIP1-A\_4228 Angaben in der Beantragung eines CVC-CA-Zertifikats**

Mit der Beantragung eines CVC-CA-Zertifikats bei der CVC-Root-CA MUSS der TSP-CVC die folgenden Angaben bereitstellen:   
(a) Name und Anschrift der CVC-CA,   
(b) CA-Name im Zertifikat (5 ASCII-Zeichen),   
(c) Typ des gewünschten Zertifikats (produktive CVC-CA oder Test-CVC-CA),   
(d) Name und Vorname einer Kontaktperson,   
(e) Fingerprint über den öffentlichen Schlüssel, für den das CVC-CA-Zertifikat erzeugt werden soll,   
(f) Unterschriften zweier hierfür berechtigter Mitarbeiter des TSP-CVC.

**⌫**

**⌦ TIP1-A\_2655 Konsistenz des CA-Namens**

Der TSP-CVC MUSS sicherstellen, dass die Angaben zu "Name und Anschrift der CVC-CA" sowie "CA-Name im Zertifikat" identisch sind zu seinen Angaben in der Registrierung bzw. der zugehörigen letzten Änderungsmitteilung.

**⌫**

**⌦ TIP1-A\_2656 Beantragung und Rollen**

Der TSP-CVC MUSS bei der Beantragung eines CVC-CA-Zertifikats Kontaktper­sonen angeben, die im Rahmen der Zulassung (oder einer Änderung) angegeben wurden und eine der Rollen "Leiter CA", "Sicherheitsbeauftragter" bzw. "Antragsteller CVC-CA-Zertifikat" inne haben. Der TSP-CVC MUSS sicherstellen, dass eine der Unterschriften von einem Mitarbeiter stammt, dem die Rolle "Leiter CVC-CA" zugewiesen wurde. Weiterhin MUSS der TSP-CVC sicherstellen, dass die zweite Unterschrift von einem weiteren bei der Zulassung bzw. einer Änderungs­mitteilung genannten Mitarbeiter ("Sicherheitsbeauftragter" bzw. "Antragsteller CVC-CA-Zertifikat") stammt.

**⌫**

Nach Eingang eines schriftlichen Antrags prüft der Anbieter der CVC-Root-CA den eingegangenen Antrag. Grundlage für die Überprüfungen ist die aktuelle Liste mit den zugelassenen TSP-CVCs und registrierten CVC-CAs, die die gematik dem Anbieter der CVC-Root-CA regelmäßig zur Verfügung stellt.

Haben alle Überprüfungen ein positives Ergebnis, bestätigt der Anbieter der CVC-Root-CA schriftlich dem TSP-CVC den Antrag und teilt dabei den Termin mit, an dem das eigentliche Zertifikat erzeugt werden soll.

Die CVC-Root-CA wird nur dann ein CVC-CA-Zertifikat für die CVC-CA ausstellen, falls der CVC-PKCS#10-Request persönlich durch einen hierfür vorher genannten Mitarbeiter überbracht wird.

Hat eine der Überprüfungen ein negatives Ergebnis, wird der Antrag durch den Anbieter der CVC-Root-CA abgelehnt. Der TSP-CVC wird entsprechend schriftlich informiert.

**⌦ TIP1-A\_2657 Korrektheit der Angaben**

Der TSP-CVC MUSS die Korrektheit der Werte in seinem Request für ein CV-Zertifikat sicherstellen.

**⌫**

Der Anbieter der CVC-Root-CA übernimmt die angegebenen Werte in das CV-Zertifikat der CVC-CA.

**⌦ TIP1-A\_2658 Nutzung der Schnittstelle zur Beantragung eines CVC-CA-Zertifikats**

Zur Nutzung der Schnittstelle bzw. zur Durchführung der Beantragung eines CVC-CA-Zertifikats MÜSSEN durch die CVC-CA die folgenden Schritte durchgeführt werden:   
(1) Das Formular zur Beantragung eines CVC-CA-Zertifikats wird von den Web-Seiten des Anbieters der CVC-Root-CA heruntergeladen, ausgefüllt und (handschriftlich) unterschrieben. Dieses Formular wird an den Anbieter der CVC-Root-CA gesendet.   
(2) Nach positiver Prüfung des Antrags durch den Anbieter der CVC-Root-CA erhält der TSP-CVC den Termin mitgeteilt, an dem das CVC-CA-Zertifikat erzeugt werden soll.   
(3) Falls bisher noch nicht geschehen, MUSS die Schlüsselgenerierung für die CVC-CA durch den TSP-CVC vorgenommen werden.   
(4) Der TSP-CVC erzeugt für das Schlüsselpaar einen Request.   
(5) Der Request MUSS gesichert durch einen dazu berechtigten Mitarbeiter des TSP-CVC persönlich an den vereinbarten Termin an die CVC-Root-CA überbracht werden.   
(6) Nach Erzeugung des CVC-CA-Zertifikats durch die CVC-Root-CA wird das Zertifikat unter Anwendung des Vier-Augen-Prinzips in die Systeme des TSP-CVC eingebracht.   
(7) Die (nicht) erfolgreiche Durchführung des Prozesses MUSS einschließlich der Beantragung durch den TSP-CVC dokumentiert und revisionssicher aufbewahrt werden.

**⌫**

**⌦ TIP1-A\_2659 Name der CA**

Jede produktive und jede Test-CVC-CA MUSS einen innerhalb einer Kartenge­neration eindeutigen CA-Namen (5 ASCII-Zeichen) verwenden. Dabei gilt:   
(a) Bei einer in Deutschland betriebenen CVC-CA MUSS der CA-Name bei der hierfür durch den DIN beauftragten Registrierungsstelle (Fraunhofer Gesellschaft SIT) registriert sein.   
(b) Bei einer außerhalb Deutschlands betriebenen CVC-CA MUSS der CA-Name bei der jeweils zuständigen nationalen Registrierungsstelle registriert sein.

**⌫**

Bisherige Kennungen und Antragsformular stehen unter [www.sit.fraunhofer.de](http://www.sit.fraunhofer.de). Diese CA-Namen beginnen mit den zwei Zeichen DE.

**⌦ TIP1-A\_2660 CA-Namen bei Betrieb mehrerer CVC-CAs**

Hat ein TSP-CVC verschiedene CVC-CAs, mit denen er CV-Zertifikate für ver­schiedene Kartengenerationen erzeugt, so KÖNNEN diese CVC-CAs den gleichen CA-Namen haben.

**⌫**

**⌦ TIP1-A\_3029 Name einer Test-CVC-CA**

Der TSP-CVC MUSS sicherstellen, dass die CA-Namen für Test-CVC-CA und der produktiven CVC-CA unterschiedlich sind sowie der CA-Name für die Test-CVC-CA ein X enthält.

**⌫**

**⌦ TIP1-A\_2696 Sicherstellung der Zuordnung von CV-Zertifikaten bei mehreren CVC-CAs mit gleichem Namen**

Sofern ein TSP-CVC verschiedene CVC-CAs mit gleichem CA-Namen betreibt, MUSS er über die Belegung des Feldes Certificate Authority Reference (CAR) sicherstellen, dass die erzeugten CV-Zertifikate eindeutig der ausgebenden CVC-CA zugeordnet werden können.

**⌫**

*Hinweis: Die technischen Details der Schnittstelle P\_Sub\_CA\_Certification\_CVC sind in gemSpec\_CVC\_Root im Kapitel 6.1 beschrieben. Zur Vermeidung von Redundanzen wird daher der nachfolgende Block entfernt.*

## Unterscheidung produktiver CVC-CA und Test-CVC-CA

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

**⌦ TIP1-A\_3030 Betrieb von Test-CVC-CAs**

Jeder TSP-CVC der zweiten Ebene MUSS neben einer produktiven CVC-CA ebenfalls eine Test-CVC-CA betreiben.

**⌫**

Der TSP-CVC 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#3.6]).

**⌦ TIP1-A\_3031 Registrierung einer Test-CVC-CA**

Der TSP-CVC MUSS eine Test-CVC-CA bei der gematik registrieren.

**⌫**

Die Qualifizierung einer Test-CVC-CA, die zur Ausgabe von Test-CV-Zertifikaten mit Rollen­profil ungleich 0 und 8 vorgesehen ist, ist nicht erforderlich.

Die Prozesse zur Beantragung eines „Test-CVC-CA-Zertifikats“ sowie zur Ausgabe von „Test-CV-Zertifikaten“ sind für die produktive CVC-CA und für die Test-CVC-CA identisch.

# Funktionsmerkmale

Ein Antrag für ein CV-Zertifikat für eine Chipkarte (eGK, HBA, SM-B, gSMC) darf nur durch den Herausgeber dieser Chipkarte oder. durch einen von diesem benannten Dritten gestellt werden. Der Antrag muss bei dem TSP-CVC gestellt werden. Details dieses Vorgangs müssen zwischen Kartenherausgeber, CVC-CA und Kartenpersonalisierergeregelt werden (sofern der Kartenherausgeber diese Funktionen nicht selbst ausführt). Grundlegende Anforderungen hierzu siehe Abschnitt 4.5.

Bei der Generierung eines CV-Zertifikats müssen die Anforderungen aus Kapitel 4 eingehalten werden.

Nach der Generierung muss das CV-Zertifikat in die zugehörige Chipkarte eingebracht werden (Staging). Die hierfür notwendigen Prozesse müssen bilateral zwischen der CVC-CA und dem Kartenpersonalisierer festgelegt werden. Grundlegende Anforderungen hierzu siehe Abschnitt 4.5.

CV-Zertifikate können gemäß [gemKPT\_PKI\_TIP#5.5] nicht gesperrt werden. Muss die Einsetzbarkeit eines CV-Zertifikatsbei Vorliegen eines schwer­wiegen­den Problems beendet werden, kann dies nur durch Einziehen und Zerstören der zugehörigen Chipkarte erreicht werden.

## Ausstellung von CV-Kartenzertifikaten durch CVC-CA

**⌦ TIP1-A\_2665 Berechtigung des Antragstellers für CV-Zertifikate**

Der TSP CVC MUSS den Herausgabeverantwortlichen gemäß Kapitel 1.6 als berechtigte Antragsteller von CV-Zertifikaten authenti­fizieren. D.h. die CVC-CA erzeugt nur dann die beantragten CV-Zertifikate, sofern die Be­rechtigung des Antragstellers erfolgreich verifiziert werden konnte.

**⌫**

**⌦ TIP1-A\_2666 Schriftliche Beantragung von CV-Zertifikaten durch einen Karten­herausgeber**

Die Beantragung von CV-Zertifikaten durch den Herausgabeverantwortlichen gemäß Kapitel 1.6 bei dem TSP-CVC MUSS bei dem TSP CVC dokumentiert werden.

**⌫**

Entsprechende Informationen werden auf den Web-Seiten der gematik zur Verfügung gestellt und regelmäßig aktualisiert.

### Schnittstelle P\_CVC\_Provisioning

#### Schnittstellendefinition

**⌦ TIP1-A\_2668 Zur Verfügung gestellte Eingangsdaten zur Erzeugung von CV-Zertifikaten**

Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS pro CV-Zertifikat mindestens die folgenden Ein­gangs­daten für CV-Zertifikate zur Verfügung stellen:  
(a) Öffentlicher Schlüssel   
(b) Card Holder Referenz, CHR, bestehend aus ’xx xx’ || ICCSN der Chipkarte (der Wert ’xx xx’ wird durch die einzelnen konkreten Chipkartenspezifikationen der gematik festgelegt und in Tabelle gemSpec\_PKI#TAB\_PKI\_258 dargestellt.)   
(c) Card Holder Authorization, CHA, bestehend aus Application Identifier (AID) || Zugriffsprofil („||“ steht für die Konkatenation von Datenelementen) für CV-Zertifikate der Kartengeneration 1 oder   
CHAT für CV-Zertifikate der Kar­tengeneration 2   
(d) Typ des CV-Zertifikats (Test oder produktiv).

**⌫**

**⌦ TIP1-A\_2669 Ausgangsdaten der CV-Zertifikatserzeugung, die durch die CVC-CA zur Verfügung gestellt werden**

Durch die CVC-CA MÜSSEN für jedes erzeugte CV-Zertifikat mindestens die fol­gen­den Daten an den Herausgabeverantwortlichen gemäß Kapitel 1.6 zurückgegeben werden:   
(a) Erzeugtes CV-Zertifikat,   
(b) CV-Zertifikat der CVC-CA.

**⌫**

Die CVC-CA muss ihr aktuelles CVC-CA-Zertifikat den Kartenpersonalisierern zur

**⌦ TIP1-A\_2671 Anforderungen an die Datenintegrität und -authentizität**

Für den Datenaustausch mit dem Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS der TSP-CVC einen Mechanismus zur Sicherung der Datenintegrität und -authentizität zur Verfügung stellen.

**⌫**

Zur Sicherung der Datenintegrität und -authentizität können Mechanismen auf Basis sym­metrischer oder asymmetrischer Kryptographie eingesetzt werden. Hierbei sind die Anfor­derungen zur Verwendung kryptographischer Algorithmen in der Telematikinfrastrukur zu berücksichtigen [gemSpec\_Krypt].

**⌦ TIP1-A\_2672 Anforderungen an die Vertraulichkeit**

Für den Datenaustausch mit dem Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS der TSP-CVC einen Mechanismus zur Verschlüsselung der Daten zur Verfügung stellen.

**⌫**

Zur Wahrung der Vertraulichkeit können Mechanismen auf Basis symmetrischer oder asym­metrischer Kryptographie eingesetzt werden. Hierbei sind die Anforderungen zur Verwendung kryptographischer Algorithmen in der Telematikinfrastrukur zu berücksich­tigen [gemSpec\_Krypt].

#### Umsetzung

Der TSP-CVC nimmt die Eingangsdaten des Herausgabeverantwortlichen gemäß Kapitel 1.6 entgegen und erzeugt die beauftragten CV-Zertifikate. Pro Datensatz des Herausgabeverantwortlichen gemäß Kapitel 1.6 zu einem öffentlichen Schlüssel (öffentlicher Schlüssel, CHR und CHA bzw. CHAT) werden die erforderlichen Angaben zu einem CV-Zertifikat zusammengestellt. Hierzu gehören die Daten gemäß [gem­Spec\_PKI#6.4] und [gem­Spec\_PKI#6.7].

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

**⌦ TIP1-A\_2673 Berücksichtigung von Eingangsdaten gemäß [gemSpec\_PKI]**

Für die Erzeugung des Zertifikats MUSS der TSP-CVC 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\_2676 Verwendung der Eingangsdaten**

Der TSP-CVC MUSS zur Erzeugung eines CV-Zertifikats die zur Verfügung gestellten Daten verwenden.

**⌫**

**⌦ TIP1-A\_5378 Setzen der Certificate Effective Date (CED)**

Der TSP-CVC (ausgenommen der TSP-CVC eGK) MUSS bei Erzeugung eines CV-Zertifikats für die Karten­ge­nera­tion 2~~,~~ als Certificate Effective Date (CED) ein durch den Kartenherausgeber oder durch einen von ihm benannten Dritten definiertes Startdatum eintragen. Für Komponentenzertifikate wird das Startdatum durch den TSP-CVC festgelegt.

**⌫**

**⌦ TIP1-A\_5379 Setzen der Certificate Expiration Date (CXD)**

Der TSP-CVC MUSS bei Erzeugung eines CV-Zertifikats für die Karten­ge­neration 2 als Certificate Expiration Date (CXD) ein Datum einstellen, das die Gül­tig­keitsdauer des CV-Zertifikats in Abhängigkeit der Kartenart festlegt und die in Tab\_PKI\_950 de­finierten maximalen Gültigkeitsdauern einhält.

**⌫**

Tabelle 1: Tab\_PKI\_950 Maximale Gültigkeitsdauern von CV-Zertifikaten

|  |  |
| --- | --- |
| **Kartentyp** | **Maximale Gültigkeitsdauer** |
| eGK | 5 Jahre |
| HBA | 5 Jahre |
| SMC-B | 5 Jahre |
| HSM-B | 5 Jahre |
| SMC-K | 5 Jahre |
| SMC-KT | 5 Jahre |

**⌦ TIP1-A\_2677 Signierung des CV-Zertifikats durch die CVC-CA**

Die zusammengestellten Daten für das CV-Zertifikat, das für einen Einsatz in der Produktivumgebung vorgesehen ist, MÜSSEN durch die produktive CVC-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.

### Artefakte

#### Card Holder Reference

Die Card Holder Reference (CHR) besteht aus der Konkatenation eines Wertes zur Identifizierung des Schlüssels sowie der ICCSN der Chipkarte, d.h.

CHR = ’xx xx’ || ICCSN der Chipkarte.

Die ICCSN ist 10 Byte lang und identifiziert eine Chipkarte eindeutig.

CV-Zertifikate der Kartengeneration 2 enthalten die CHR in einem eigenen Datenobjekt (vgl. Kapitel 5.1.2.4).

**⌦ TIP1-A\_2678 Identifizierung eines HSM-B**

Wird anstelle einer SMC-B ein HSM-B eingesetzt, MUSS durch den Karten­personalisierer sichergestellt werden, dass eine dem Format der ICCSN entsprechende eindeutige Identifikation des HSM-B zur Verfügung gestellt wird.

**⌫**

Eine Chipkarte kann auch mehrere Schlüsselpaare für eine C2C-Authentisierung (und damit auch mehrere CV-Zertifikate) enthalten. Über die konkrete Belegung von 'xx xx' muss sichergestellt werden, dass die Zuordnung von CV-Zertifikat zu einem Schlüssel­paar der Chipkarte eindeutig ist. Das genaue Vorgehen hierbei wird durch die einzelnen konkreten Chipkartenspezifikationen der gematik festgelegt.

#### Card Holder Authorization

Die Card Holder Authorization (CHA) besteht aus der Konkatenation der Parameter AID und dem Zugriffsprofil, d.h. CHA = AID || Zugriffsprofil.

Die AID ist 6 Bytes lang. Es muss die AID der Gesundheitskartenanwendung 'D2 76 00 00 40 00' eingetragen werden.

Das Zugriffsprofil wird in einem Byte kodiert.

CV-Zertifikate der Kartengeneration 2 enthalten anstelle der CHA das Card Holder Authorization Template (CHAT).

#### Certificate Authority Reference

CV-Zertifikate der Kartengeneration 2 enthalten die CAR in einem eigenen Datenobjekt (vgl. Kapitel 5.1.2.4).

**⌦ TIP1-A\_2680 Eindeutigkeit der Zuordnung zwischen CAR und Schlüsselpaar der CVC-CA**

Der TSP-CVC MUSS sicherstellen, dass die Zuordnung zwischen Certificate Authority Reference (CAR) und Schlüsselpaar eindeutig ist.

**⌫**

#### Datenobjekte eines CV-Zertifikats der Generation 2

Alle Angaben in einem CV-Zertifikat der Kartengeneration 2 erfolgen über eigene Daten­ob­jekte. Hierzu gehören die Angaben zu CPI, CAR, öffentlicher Schlüssel, CHR, dem Certificate Holder Authorization Template (CHAT), Ausstellungsdatum und Gültigkeits­ende sowie die Signatur über die Inhalte des CV-Zertifikats. Das Zertifikatsprofil eines CV-Zertifikats der Kartengeneration 2 ist in [gemSpec\_PKI#6.7] beschrieben.

### Testunterstützung

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

**⌦ TIP1-A\_3032 Signierung des Test-CV-Zertifikats durch die Test-CVC-CA**

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

**⌫**

**⌦ TIP1-A\_4229 Optionale Sicherheitsmechanismen bei Ausgabe von Test-CV-Zertifikaten**

Der TSP-CVC KANN für den Datenaustausch bei der Ausgabe von Test-CV-Zer­tifikaten auf den Einsatz von Mechanismen zur Sicherung der Datenintegrität und   
-authentizität sowie zur Verschlüsselung von Daten verzichten.

**⌫**

# 

# Anhang A – Verzeichnisse

## A1 – Abkürzungen

| **Kürzel** | **Erläuterung** |
| --- | --- |
| C2C | Card to Card |
| CA | Certification Authority |
| CAR | Certificate Authority Reference |
| CHA | Certificate Holder Authorization |
| CHAT | Certificate Holder Authorization 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 |
| 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 |
| HPC | Health Professional Card |
| HSM | Hardwaresicherheitsmodul |
| ICCSN | ICC Serial Number |
| KTR | Kostenträger |
| LEO | Leistungserbringerorganisation |
| OID | Object Identifier |
| PKI | Public Key Infrastructure |
| PrK | Private Key |
| PuK | Public Key |
| PTB | Physikalisch-Technische Bundesanstalt |
| RFC | Request For Comment |
| RSA | Algorithmus benannt nach Rivest, Shamir und Adleman |
| SGB | Sozialgesetzbuch |
| 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: Nachbarsysteme eines TSP-CVC eGK 13](#_Toc480470595)

## A4 – Tabellenverzeichnis

[Tabelle 1: Tab\_PKI\_950 Maximale Gültigkeitsdauern von CV-Zertifikaten 36](#_Toc457399345)

## 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 |
| [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. |

1. Gemäß Kapitel 2.7.3.4 aus [gemKPT\_PKI\_TIP] [↑](#footnote-ref-2)