Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation

Trust Service Provider CVC

Version:	1.5.0
Revision:	\main\rel_online\rel_ors1\13
Stand:	17.06.2014
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_CVC_TSP]

Dokumentinformationen

Änderungen zur Vorversion

Die Anforderung TIP-A-2692 wurde neu formuliert.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	26.07.12		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentierung Gesellschafter	P77
1.0.0	15.10.12		freigegeben	gematik
			Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	P77
1.1.0	12.11.12		freigegeben	gematik
	15.02.13		Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen)	P77
1.1.9	22.04.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare aus Kommentierung Gesamtpaket	P77
1.2.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.2.0	06.06.13		freigegeben	gematik
			Einarbeitung Kommentare Änderungsliste	P77
1.3.0	18.12.13		freigegeben	gematik
			Losübergreifende Synchronisation	P77
1.4.0	21.02.14		freigegeben	gematik
	17.04.14		Die Anforderung TIP-A-2692 wurde neu formuliert	P77
1.5.0	17.06.14		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einordnung des Dokumentes 5

1.1 Zielsetzung 5

1.2 Zielgruppe 5

1.3 Geltungsbereich 5

1.4 Abgrenzungen 5

1.5 Methodik 6

2 Systemüberblick 7

2.1 Hierarchie der PKI für CV-Zertifikate 7

2.2 Begriffsverwendung 7

3 Systemkontext 9

3.1 Akteure und Rollen 9

3.1.1 Anbieter der CVC-Root-CA 9

3.1.2 Kartenherausgeber 10

3.1.3 TSP-CVC 10

3.1.4 Kartenhersteller 11

3.1.5 Zertifikatsnehmer 11

3.1.5.1 Karteninhaber (eGK) *11*

3.1.5.2 Karteninhaber (HBA, SM-B) *12*

3.1.5.3 Karteninhaber (gSMC) *12*

3.2 Nachbarsysteme 12

3.3 Zugriffsprofile 13

3.4 Sperren und Nachladen von CV-Zertifikaten der Karten- generation 2 14

4 Übergreifende Festlegungen 15

4.1 Erstellung Ausgabepolicy durch TSP-CVC 15

4.2 Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-CVC 15

4.3 Zulassung 16

4.4 Registrierung und Qualifizierung 16

4.5 Zusammenspiel Kartenherausgeber, CVC-CA und Kartenhersteller 17

4.6 Mindestanforderungen an eine CVC-CA 20

4.6.1 Schutzbedarfsfeststellung 20
4.6.2 Verfügbarkeit der CVC-CA 21
4.6.3 Ausschließlichkeit und Dauer der Schlüsselnutzung 21
4.6.4 Verlust der Zulassung 22
4.6.5 Sicherheit des Schlüsselpaares 22
4.6.6 Algorithmen und Schlüssellängen 25
4.6.7 Schlüsselversionen 25
4.6.8 Protokollierung 26
4.6.9 Personelle Anforderungen 27
4.6.10 Betriebliche Anforderungen 28
4.6.11 Authentizität des öffentlichen Schlüssels der CVC-CA 29
4.6.12 Synchronisierung mit dem Zeitdienst 30

4.7 Beantragung eines CV-Zertifikats für die CVC-CA 30

4.8 Unterscheidung produktiver CVC-CA und Test-CVC-CA 32

5 Funktionsmerkmale 34

5.1 Ausstellung von CV-Kartenzertifikaten durch CVC-CA 34
5.1.1 Schnittstelle P_CVC_Provisioning 35
5.1.1.1 Schnittstellendefinition 35
5.1.1.2 Umsetzung 36
5.1.2 Artefakte 37
5.1.2.1 Card Holder Reference 37
5.1.2.2 Card Holder Authorisation 37
5.1.2.3 Certificate Authority Reference 38
5.1.2.4 Datenobjekte eines CV-Zertifikats der Generation 2 38
5.1.3 Testunterstützung 38

Anhang A – Verzeichnisse 40

A1 – Abkürzungen 40

A2 – Glossar 41

A3 – Abbildungsverzeichnis 41

A4 – Tabellenverzeichnis 41

A5 - Referenzierte Dokumente 41
A5.1 – Dokumente der gematik 41
A5.2 – Weitere Dokumente 42

1 Einordnung des Dokumentes

1.1 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 beschrieben.

1.2 Zielgruppe

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

1.3 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.

1.4 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.

Anmerkung: Für die Kartengeneration 2 verfügen CV-Zertifikate über einen Gültigkeitszeitraum, in dem der Ausgabezeitpunkt sowie das Gültigkeitsende des CV-Zertifikats angegeben werden. Der TSP-CVC erneuert diese CV-Zertifikate solange bis entweder das Ende der Kartenlaufzeit erreicht ist oder die Erneuerung im Sinne einer Sperrung unterbunden wird. Die aktuell vorliegende Spezifikation enthält Anforderungen an einen TSP-CVC zur Ausgabe von CV-Zertifikaten der Kartengeneration 2, die Definition der Schnittstelle zur Erneuerung von CV-Zertifikaten wird jedoch zu einem späteren Zeitpunkt ergänzt.

Die Schnittstelle für die Erneuerung der CV-Zertifikate der Kartengeneration 2 ist noch nicht Bestandteil der aktuell vorliegenden Spezifikation. Die Definition dieser Schnittstelle wird zu einem späteren Zeitpunkt ergänzt.

1.5 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.

2 Systemüberblick

2.1 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 von Kartenherstellern, ZDAs 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.

2.2 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. Analog wird gSMC als Oberbegriff verwendet, wenn die Differenzierung zwischen gSMC-K und gSMC-KT nicht erforderlich 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.

3 Systemkontext

3.1 Akteure und Rollen

An der PKI für CV-Zertifikate sind verschiedene Organisationen bzw. Personen beteiligt. 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.

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.

3.1.1 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.

3.1.2 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 eine bei der gematik vorgenommene Registrierung sowie ggf. über eine Qualifizierung seitens der kartenherausgebenden Organisation.

Der Kartenherausgeber muss, in Zusammenarbeit mit dem Kartenhersteller 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.

Für die Ausgabe von HBAs und SM-Bs können weitere Anforderungen durch die jeweils zuständige Standesorganisation der Leistungserbringer vorgegeben werden.

Der Kartenherausgeber kann seine Verantwortlichkeiten nur in Zusammenarbeit mit dem Kartenhersteller und dem TSP-CVC erfüllen. Siehe dazu Abschnitt 4.5.

3.1.3 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) 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-Zertifikate 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]).

3.1.4 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. die folgenden Werte in die Chipkarte ein:

- aktueller öffentlicher Schlüssel der CVC-Root-CA,
- CVC-CA-Zertifikat der CVC-CA, die das CV-Zertifikat (bzw. die CV-Zertifikate) für die Chipkarte generiert hat,
- ggf. mehrere CV-Zertifikate der Chipkarte,
- der (bzw. die) private(n) Schlüssel, dessen (deren) öffentlicher Schlüssel durch das CV-Zertifikat bzw. die CV-Zertifikate zertifiziert wird (werden).

Der Kartenhersteller, in Zusammenarbeit mit dem Kartenherausgeber und der CVC-CA, stellt sicher, dass hierbei die korrekten Werte in die Chipkarte eingebracht werden (siehe Abschnitt 4.5).

Chipkarten, die vor Weitergabe als fehlerhaft erkannt werden, werden durch den Kartenhersteller ordnungsgemäß entsorgt.

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

3.1.5 Zertifikatsnehmer

3.1.5.1 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.

3.1.5.2 Karteninhaber (HBA, SM-B)

Ein HBA bzw. eine SM-B enthält ein CV-Rollen-Zertifikat 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.

⌦ **TIP1-A_2555 Meldepflicht des Karteninhabers HBA (Sicherheitsmodul vom Typ B)**

Im Rahmen der PKI für CV-Zertifikate MUSS der Kartenherausgeber sicherstellen, dass ein Inhaber eines HBA bzw. eines Sicherheitsmoduls vom Typ B jede Änderung seiner Zugehörigkeit zu der für die Ausgabe seines HBA relevanten Berufsgruppe sowie den Verlust seines HBA unverzüglich seiner für die Ausgabe des HBA bzw. des Sicherheitsmoduls zuständigen Standesorganisation der Leistungserbringer bzw. dem Kostenträger meldet. ⌫

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

Ein HBA enthält zusätzlich zu dem CV-Rollen-Zertifikat auch ein CV-Geräte-Zertifikat. Aus dessen Existenz ergeben sich keine weiteren Pflichten für den Karteninhaber.

3.1.5.3 Karteninhaber (gSMC)

Eine gSMC enthält nur ein CV-Geräte-Zertifikat. Durch eine C2C-Authentisierung mit einer anderen Chipkarte erhält die gSMC und damit ihr Karteninhaber keine weiteren Zugriffsrechte auf in der anderen Chipkarte gespeicherte Daten.

⌦ **TIP1-A_2556 Meldepflicht des Karteninhabers einer gerätebezogenen SMC**

Im Rahmen der PKI für CV-Zertifikate MUSS der Kartenherausgeber sicherstellen, dass ein Inhaber einer gerätebezogenen SMC-K den Verlust seiner Karte unverzüglich dem Gerätehersteller als kartenausgebende Organisation meldet. ⌫

Konkrete Festlegungen hierzu werden durch den Gerätehersteller geregelt.

Bei Verlust einer gSMC-KT sollte dem Leistungsbringer empfohlen werden, seine Signatur-PIN (zur Erstellung qualifizierter Signaturen mit dem HBA) zu wechseln. Eine entsprechende Empfehlung könnte beispielsweise in der HPC-Policy aufgenommen werden. Hintergrund ist die Verschlüsselung der Signatur-PIN in der gSMC-KT bei Anwendung des Remote-PIN-Verfahrens.

3.2 Nachbarsysteme

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

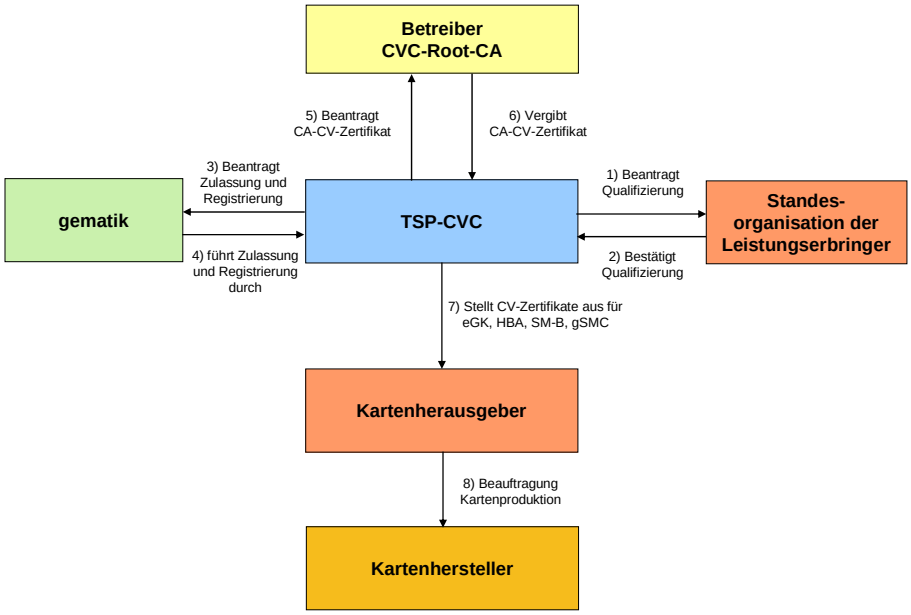

Abbildung 1: Nachbarsysteme eines TSP-CVC

Die Qualifizierung eines TSP-CVC 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. Eine Qualifizierung für die Ausgabe von CV-Rollen-Zertifikaten mit dem Zugriffsprofil 0 (eGK) oder 8 (SM-B) ist nicht notwendig.

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 beauftragt den Kartenhersteller mit der Produktion (Personalisierung) der Karten (Schritt 8).

3.3 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 ’01’) 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 bzw. ’01’ für CV-Rollen-Zertifikat oder Rolle 51 bzw. ’33’ für ein 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].

3.4 Sperren und Nachladen von CV-Zertifikaten der Kartengeneration 2

CV-Zertifikate der Kartengeneration 2 enthalten einen Ausgabezeitpunkt sowie ein Gültigkeitsende. Nur in diesem zeitlich eingegrenzten Bereich ist eine C2C-Authentisierung erfolgreich möglich. Wird beabsichtigt, dem Zertifikatsinhaber auch nach Gültigkeitsende weiterhin die im CV-Zertifikat enthaltene Rolle zuzuweisen, so ist ein neues CV-Zertifikat auf Basis des bestehenden Schlüsselpaars auszustellen, welches sich vom alten CV-Zertifikat nur durch geänderte Gültigkeitszeitpunkte unterscheidet.

Die Neuausstellung der CV-Zertifikate wird auch als Zertifikatserneuerung bezeichnet.

Eine Sperrung von CV-Zertifikaten ist nicht vorgesehen.

Aus Sicht einer CVC-CA werden solange neue CV-Zertifikate für einen dedizierten öffentlichen Schlüssel erstellt und zur Distribution angeboten, bis das Ende der Kartengültigkeit erreicht ist oder die weitere Zertifikatserneuerung unterbunden wird. Letzteres entspricht einer „Sperrung“ des Schlüsselpaares.

Für neu ausgestellte Karten müssen in jedem Fall neue Schlüsselpaare generiert werden.

Ein Gültigkeitsende für die CV-Zertifikate der Kartengeneration 2 ist nur für Karten sinnvoll, die mit Zugriffsrechten auf andere Karten ausgestattet sind, um damit deren Missbrauchspotential einzugrenzen. Da die eGK über keine Zugriffsrechte verfügt, muss das Ablaufdatum gleich dem Ende der Kartengültigkeit gesetzt werden.

4 Übergreifende Festlegungen

4.1 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. ⌫

4.2 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 von Kartenherausgeber, Kartenhersteller und CVC-CA im Sicherheitskonzept**

In dem Sicherheitskonzept des TSP-CVC MUSS der TSP-CVC beschreiben, wie die Zusammenarbeit von Kartenherausgeber, Kartenhersteller und CVC-CA organisiert ist und wie die entsprechenden Sicherheitsmaßnahmen bei den einzelnen Organisationen greifen. ⌫

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

4.3 Zulassung

⌦ **TIP1-A_2562 Ausstellung von CVC-CA-Zertifikate für zugelassene TSP-CVC**

Der Anbieter der CVC-Root-CA MUSS sicherstellen, dass ein CV-Zertifikat für eine CVC-CA nur dann erzeugt wird, wenn der TSP-CVC aktuell bei der gematik zugelassen ist. Eine Ausnahme hiervon ist nicht möglich. ⌫

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

- Kartenherausgeber,
- Kartenhersteller,
- Kartenpersonalisierer,
- ZDAs im Sinne von SigG.

⌦ **TIP1-A_2563 Hauptsitz und Betriebsstätte des TSP-CVC**

Der TSP-CVC MUSS seinen Hauptsitz und die Betriebsstätte für den tatsächlichen Betrieb in einem Land der Europäischen Union haben. ⌫

4.4 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. ⌫

Durch die Qualifizierung bestätigt die Standesorganisation der Leistungserbringer, dass die CVC-CA alle gestellten Anforderungen erfüllt.

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. ⌫

Alle Anforderungen an eine CVC-CA für eine Qualifizierung sowie das Vorgehen für ihre Durchführung werden durch die zuständige Standesorganisation der Leistungserbringer geregelt.

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

4.5 Zusammenspiel Kartenherausgeber, CVC-CA und Kartenhersteller

Bei dem Prozess für die Herstellung einer Chipkarte (eGK, HBA, SM-B, gSMC) müssen Kartenherausgeber, Kartenhersteller, CVC-CA und CAs anderer PKI zusammenarbeiten. Die genaue Aufgabenteilung wird nicht einheitlich vorgegeben. Bei der Produktion verschiedener Karten sind unterschiedliche Formen der Zusammenarbeit und der Aufgaben-

teilung denkbar. Dabei obliegt die technische Durchführung der in den folgenden Anforderungen enthaltenen Aufgaben i.d.R. dem Kartenhersteller. 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_2574 Beauftragung der Kartenproduktion**

Der Kartenherausgeber MUSS die Produktion einer Chipkarte mit zugehörigem CV-Zertifikat beauftragen. ⌫

⌦ **TIP1-A_2575 Zugelassenes Zugriffsprofil im CV-Rollen-Zertifikat**

Der Kartenherausgeber und Kartenhersteller MÜSSEN 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. ⌫

⌦ **TIP1-A_2576 Zugelassenes Zugriffsprofil im CV-Geräte-Zertifikat**

Der Kartenherausgeber und Kartenhersteller MÜSSEN sicherstellen, dass in einem CV-Geräte-Zertifikat einer Chipkarte ein bestimmtes Zugriffsprofil genau dann kodiert wird, falls das Gerät, die entsprechende Funktionseinheit unterstützt. ⌫

⌦ **TIP1-A_2577 Zugelassenes Zugriffsprofil in der Chipkarte einer Funktionseinheit Signaturanwendungskomponente**

Der Kartenherausgeber und Kartenhersteller MÜSSEN sicherstellen, dass in einem CV-Geräte-Zertifikat einer Chipkarte nur dann das Zugriffsprofil einer Signaturanwendungskomponente SAK kodiert wird, falls diese Chipkarte in einen Konnektor eingebracht wird, der eine Funktionseinheit Signaturanwendungskomponente gemäß SigG/SigV unterstützt. ⌫

⌦ **TIP1-A_2578 Korrekte ICCSN der Chipkarte**

Der Kartenherausgeber und Kartenhersteller MÜSSEN 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 Kartenherausgeber und Kartenhersteller MÜSSEN sicherstellen, dass nach Produktion 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 in einem HSM**

Der Kartenherausgeber und Kartenhersteller MÜSSEN die Sicherheit des privaten Schlüssels bei dessen Erzeugung gewährleisten. Dieses bedeutet, der private Schlüssel MUSS in einem HSM generiert werden. ⌫

⌦ **TIP1-A_2581 Evaluierung von HSMs – Kartenherausgeber, Kartenhersteller**

Der Kartenherausgeber und der Kartenhersteller MÜSSEN den Einsatz eines HSM bzw. eine Chipkarte sicherstellen, deren Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Com-

mon 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 Kartenherausgeber und Kartenhersteller MÜSSEN die Vertraulichkeit des privaten Schlüssels gewährleisten. Sie MÜSSEN 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 und Kartenhersteller MÜSSEN 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), MÜSSEN Kartenherausgeber und Kartenhersteller sicherstellen, dass für jedes CV-Zertifikat ein eigenes Schlüsselpaar verwendet wird. ⌫

⌦ **TIP1-A_2585 Personalisierung von CV-Zertifikaten für einen HBA**

Bei der Personalisierung eines HBA MÜSSEN Kartenherausgeber und Kartenhersteller 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 MÜSSEN Kartenherausgeber und Kartenhersteller 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 MÜSSEN Kartenherausgeber und Kartenhersteller sicherstellen, dass das einzubringende CV-Zertifikat genau das Zugriffsprofil 0 enthält, über das keinerlei Rechte vergeben werden. ⌫

⌦ **TIP1-A_2588 Personalisierung des öffentlichen Root-Schlüssels**

Bei der Personalisierung einer Chipkarte MÜSSEN Kartenherausgeber und Kartenhersteller sicherstellen, dass der korrekte aktuelle öffentliche Schlüssel der CVC-Root-CA eingebracht wird. ⌫

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

⌦ **TIP1-A_4222 Authentizität des öffentlichen Root-Schlüssels**

Jeder Kartenherausgeber und Kartenhersteller, der den öffentlichen Schlüssel der CVC-Root-CA im Rahmen der Personalisierung verwendet, MUSS die Authentizität dieses Schlüssels vor dessen Verwendung sicherstellen. Dabei MÜSSEN Kartenherausgeber und Kartenhersteller 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 MÜSSEN Kartenherausgeber und Kartenhersteller 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**

Kartenherausgeber und Kartenhersteller MÜSSEN Chipkarten, die vor Ausgabe an den Karteninhaber als fehlerhaft erkannt werden, ordnungsgemäß vernichten. ⌫

⌦ **TIP1-A_2591 Ausgabe fehlerfreier Chipkarten**

Kartenherausgeber und Kartenhersteller MÜSSEN Chipkarten, die fehlerfrei produziert 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).

4.6 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.

4.6.1 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 geräte-bezogenen 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. ⌫

4.6.2 Verfügbarkeit der CVC-CA

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

⌦ **TIP1-A_2597 Verfügbarkeit der CVC-CA**

Der TSP-CVC MUSS sicherstellen, dass die Vorgaben an die Verfügbarkeit der CVC-CA zwischen dem die CVC-CA beauftragenden Kartenherausgeber und dem TSP-CVC geklärt werden. ⌫

4.6.3 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.

4.6.4 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. ⌫

4.6.5 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**

Falls das Klonen eines HSM technisch möglich ist, MUSS der Vorgang durch den TSP-CVC in dem Sicherheitskonzept gesondert beschrieben werden. 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 Benutzauthentisierung 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_4226 Speicherung und Auswahl von Schlüsselpaaren im HSM der CVC-CA**

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

⌦ **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. ⌫

⌦ **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. ⌫

4.6.6 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.

4.6.7 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.

4.6.8 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. ⌫

4.6.9 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) Sicherheits-

beauftragter 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. ⌫

4.6.10 Betriebliche Anforderungen

⌦ **TIP1-A_2640 Umsetzung der definierten Prozesse**

Der TSP-CVC MUSS die definierten Prozesse umsetzen. ⌫

⌦ **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. ⌫

4.6.11 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.

4.6.12 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. ⌫

4.7 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. 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.

4.8 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.

5 Funktionsmerkmale

Ein Antrag für ein CV-Zertifikat für eine Chipkarte (eGK, HBA, SM-B, gSMC) darf nur durch den Herausgeber dieser Chipkarte bzw. durch einen durch den Herausgeber beauftragten Kartenhersteller gestellt werden. Der Antrag muss bei dem TSP-CVC gestellt werden. Details dieses Vorgangs müssen zwischen Kartenherausgeber, CVC-CA und Kartenhersteller geregelt werden. 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 Kartenhersteller 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-Zertifikats der Kartengeneration 1 bei Vorliegen eines schwerwiegenden Problems beendet werden, kann dies nur durch Einziehen und Zerstören der zugehörigen Chipkarte erreicht werden. Bei CV-Zertifikaten der Kartengeneration 2 wird das im CV-Zertifikat angegebene Gültigkeitsende erreicht und das CV-Zertifikat nicht mehr erneuert.

5.1 Ausstellung von CV-Kartenzertifikaten durch CVC-CA

⌦ **TIP1-A_2665 Berechtigung des Antragstellers für CV-Zertifikate**

Die CVC-CA MUSS den Kartenherausgeber bzw. den Antragsberechtigten des Kartenherausgebers als berechtigten 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 einen Kartenherausgeber bei der CVC-CA MUSS schriftlich erfolgen und bei der CVC-CA dokumentiert werden. ⌫

⌦ **TIP1-A_2667 Sicherstellung der Eignung der CVC-CA durch den Kartenherausgeber**

Vor der Beantragung von CV-Zertifikaten MUSS sich der Kartenherausgeber darüber informieren, ob der TSP-CVC über die erforderliche Zulassung und die CVC-CA über die erforderliche Registrierung verfügt. Weiterhin MUSS der Kartenherausgeber prüfen, ob die CVC-CA über eine Qualifizierung verfügt, sofern CV-Zertifikate mit spezifischen Profilen beantragt werden sollen. ⌫

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

5.1.1 Schnittstelle P_CVC_Provisioning

5.1.1.1 Schnittstellendefinition

Die CVC-CA erstellt im Auftrage des Kartenherausgebers die CV-Zertifikate.

⌦ **TIP1-A_2668 Eingangsdaten zur Erzeugung von CV-Zertifikaten, die durch den Kartenherausgeber zur Verfügung gestellt werden**

Der Kartenherausgeber 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) (c) Card Holder Authorisation, 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). ⌫

Für die Erstellung des Zertifikats werden die durch den Kartenherausgeber zur Verfügung gestellten Eingangsdaten sowie die durch die CVC-CA verwendete Certification Authority Reference (CAR) verwendet.

⌦ **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 Kartenherausgeber zurückgegeben werden: (a) Erzeugtes CV-Zertifikat, (b) CV-Zertifikat der CVC-CA. ⌫

Die CVC-CA muss ihr aktuelles CVC-CA-Zertifikat den Kartenherstellern zur Verfügung stellen, damit dieses in die Chipkarten personalisiert werden kann.

⌦ **TIP1-A_2670 Datenaustauschformat zur Erzeugung von CV-Zertifikaten**

Der TSP-CVC MUSS sicherstellen, dass das technische Datenaustauschformat zur Erzeugung von CV-Zertifikaten bilateral zwischen Kartenherausgeber, bzw. dessen beauftragter Dienstleister, und CVC-CA vereinbart wird. Der TSP-CVC MUSS jedoch mindestens die Standards CMP und PKCS#10 unterstützen. Der TSP-CVC MUSS das Datenaustauschformat in seinem Sicherheitskonzept beschreiben und umsetzen. ⌫

⌦ **TIP1-A_2671 Anforderungen an die Datenintegrität und -authentizität**

Für den Datenaustausch mit dem Kartenherausgeber 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 Kartenherausgeber 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].

5.1.1.2 Umsetzung

Die CVC-CA nimmt die Eingangsdaten des Kartenherausgebers entgegen und erzeugt die beauftragten CV-Zertifikate. Pro Datensatz des Herausgebers 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_2674 Einschränkung der zu erzeugenden CPI**

Die CVC-CA DARF NICHT CV-Zertifikate der Kartengeneration 1 mit einem Certificate Profile Identifier (CPI) erzeugen, der von ’22’ verschieden ist. ⌫

CV-Zertifikate der Kartengeneration 1 mit einem CPI-Wert von ’22’ identifizieren CV-Zertifikate einer Chipkarte (vgl. [gemSpec_PKI#6.4]). Für CV-Zertifikate der Kartengeneration 2 wird sowohl für CVC-CA-Zertifikate als auch für CV-Zertifikate der Karten einheitlich der Wert ’70’ verwendet (vgl. [gemSpec_PKI#6.7.2.1]).

⌦ **TIP1-A_2676 Verwendung der Eingangsdaten des Kartenherausgebers**

Die CVC-CA MUSS zur Erzeugung eines CV-Zertifikats die vom Kartenherausgeber zur Verfügung gestellten Daten verwenden. ⌫

⌦ **TIP1-A_5378 Setzen der Certificate Effective Date (CED)**

Der TSP-CVC MUSS bei Erzeugung eines CV-Zertifikats für die Kartengeneration 2, solange kein Mechanismus zur Zertifikatserneuerung bereitsteht, als Certificate Effective Date (CED) das Erstellungsdatum eintragen. ⌫

⌦ **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.

5.1.2 Artefakte

5.1.2.1 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 Kartenherausgeber 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.

5.1.2.2 Card Holder Authorisation

Die Card Holder Authorisation (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 Authorisation Template (CHAT).

5.1.2.3 Certificate Authority Reference

⌦ **TIP1-A_2679 Verwendung des Feldes Certificate Authority Reference**

Die CVC-CA MUSS das Feld Certificate Authority Reference (CAR) weiter unterteilen in die Konkatenation der Datenelemente CA Name, Service-Indikator, CA-spezifische Information, Algorithmenreferenz und Datum. Für die 8 Byte lange CAR MÜSSEN die folgenden Festlegungen eingehalten werden: (a) CA Name ist 5 Byte lang. Es MUSS der CA Name eingetragen werden. (b) Service-Indikator ist eine Ziffer (4-Bit BCD-kodiert). (c) CA-spezifische Information ist eine Ziffer (4-Bit BCD-kodiert). (d) Algorithmenreferenz sind zwei Ziffern (4-Bit BCD-kodiert). (e) Datum sind zwei Ziffern (4-Bit BCD-kodiert). Es müssen die beiden letzten Ziffern des Jahres eingetragen werden, in dem das zugehörige Schlüsselpaar durch die CA aktiviert wurde. ⌫

Die Werte für Service-Indikator, CA-spezifische Information und Algorithmenreferenz kann der TSP-CVC selber festlegen.

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. ⌫

5.1.2.4 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 Authorisation 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.

5.1.3 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 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
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
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
SigG	Signaturgesetz
SigV	Signaturverordnung

© gematik – öffentlich

Kürzel	Erläuterung
SM-B	Sicherheitsmodul vom Typ B <medizinische Institution>
SMC	Security Module Card
SMC-B	SMC vom Typ B <medizinische Institution>
ZDA	Zertifizierungsdiensteanbieter

A2 – Glossar

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

A3 – Abbildungsverzeichnis

Abbildung 1: Nachbarsysteme eines TSP-CVC 13

A4 – Tabellenverzeichnis

Tabelle 1: Tab_PKI_950 Maximale Gültigkeitsdauern von CV-Zertifikaten.....37

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

[Quelle]	Herausgeber: Titel
[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.
[SigG]	Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091).