

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Trust Service Provider CVC

Version: 1.13.0 CC
Revision: 192694230687
Stand: 15.05.201930.04.2020
Status: zur Abstimmung freigegebenFreigegeben für interne QS
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_CVC_TSP

Dokumentinformationen

Änderungen zur Vorversion

~~Änderungen zur Vorversion beruhen auf P18.1, die Änderungen sind gelb markiert.~~

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0		Einarbeitung Kommentierung Gesellschafter	gematik
1.1.0		Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	gematik
1.2.0		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
1.6.1	26.05.16	Anpassungen zum Online-Produktivbetrieb (Stufe 1)	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
1.8.1	21.04.17	P14.9	gematik
1.9.0	14.05.18	Einarbeitung von P15.4	gematik
1.10.0	26.10.18	Einarbeitung von P15.9	gematik

1.11.0	18.12.18	Einarbeitung von P15.11 und P17.1	gematik
1.12.0	01.03.15 15.05.19	Einarbeitung von P18.1	gematik
1.12.13.0 CC	01.03.19 30.04.20	Anpassungen gemäß Änderungsliste P22.1 zur Abstimmung freigegeben	gematik
		Einarbeitung Kommentare	
1.12.	15.05.2019	freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes	8
1.1 Zielsetzung	8
1.2 Zielgruppe	8
1.3 Geltungsbereich	8
1.4 Abgrenzungen	8
1.5 Methodik	9
1.6 Unterscheidung der Anforderungsadressaten	9
2 Systemüberblick	10
2.1 Hierarchie der PKI für CV-Zertifikate	10
2.2 Begriffsverwendung	10
3 Systemkontext	12
3.1 Akteure und Rollen	12
3.1.1 Anbieter der CVC-Root-CA	12
3.1.2 Kartenherausgeber	13
3.1.3 TSP-CVC	13
3.1.3.1 Sektorqualifizierung	13
3.1.3.2 Sektorzulassung	14
3.1.4 Kartenpersonalisierer	14
3.1.5 Zertifikatsnehmer	14
3.1.5.1 Karteninhaber (eGK)	14
3.1.5.2 Karteninhaber (HBA, SM-B für medizinische Institutionen oder Kostenträger)	14
3.1.5.3 Karteninhaber (gSMC, SM-B für Gesellschafterorganisationen)	15
3.2 Nachbarsysteme	15
3.3 Zugriffsprofile	16
3.4 Sperren und Nachladen von CV-Zertifikaten der Karten-generation 2	17
4 Übergreifende Festlegungen	18
4.1 Erstellung Ausgabepolicy durch TSP-CVC	18
4.2 Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-CVC	18
4.3 Zulassung	19
4.4 Registrierung und Sektorqualifizierung	19
4.5 Zusammenspiel Kartenherausgeber, CVC-CA und Kartenpersonalisierer	19
4.6 Mindestanforderungen an eine CVC-CA	22
4.6.1 Schutzbedarfsfeststellung	22
4.6.2 Verfügbarkeit der CVC-CA	23
4.6.3 Ausschließlichkeit und Dauer der Schlüsselnutzung	23
4.6.4 Verlust der Zulassung	24

70	4.6.5 Sicherheit des Schlüsselpaares.....	24
71	4.6.6 Algorithmen und Schlüssellängen.....	27
72	4.6.7 Schlüsselversionen.....	28
73	4.6.8 Protokollierung.....	28
74	4.6.9 Personelle Anforderungen.....	30
75	4.6.10 Betriebliche Anforderungen.....	31
76	4.6.11 Authentizität des öffentlichen Schlüssels der CVC-CA.....	32
77	4.6.12 Synchronisierung mit dem Zeitdienst.....	32
78	4.7 Beantragung eines CV-Zertifikats für die CVC-CA.....	32
79	4.8 Unterscheidung produktiver CVC-CA und Test CVC-CA.....	35
80	5 Funktionsmerkmale.....	36
81	5.1 Ausstellung von CV-Kartenzertifikaten durch CVC-CA.....	36
82	5.1.1 Schnittstelle P_CVC_Provisioning.....	36
83	5.1.1.1 Schnittstellendefinition.....	36
84	5.1.1.2 Umsetzung.....	38
85	5.1.2 Artefakte.....	39
86	5.1.2.1 Card Holder Reference.....	39
87	5.1.2.2 Card Holder Authorization Template (CHAT).....	39
88	5.1.2.3 Certificate Authority Reference.....	39
89	5.1.2.4 Datenobjekte eines CV-Zertifikats der Generation 2.....	40
90	5.1.3 Testunterstützung.....	40
91	6 Anhang — Verzeichnisse.....	41
92	6.1 Abkürzungen.....	41
93	6.2 Glossar.....	42
94	6.3 Abbildungsverzeichnis.....	42
95	6.4 Tabellenverzeichnis.....	42
96	6.5 Referenzierte Dokumente.....	43
97	6.5.1 Dokumente der gematik.....	43
98	6.5.2 Weitere Dokumente.....	43
99	1 Einordnung des Dokumentes.....	8
100	1.1 Zielsetzung.....	8
101	1.2 Zielgruppe.....	8
102	1.3 Geltungsbereich.....	8
103	1.4 Abgrenzungen.....	8
104	1.5 Methodik.....	9
105	1.6 Unterscheidung der Anforderungsadressaten.....	9
106	2 Systemüberblick.....	10
107	2.1 Hierarchie der PKI für CV-Zertifikate.....	10
108	2.2 Begriffsverwendung.....	10
109	3 Systemkontext.....	12

110	3.1 Akteure und Rollen	12
111	3.1.1 Anbieter der CVC-Root-CA.....	12
112	3.1.2 Kartenherausgeber.....	13
113	3.1.3 TSP-CVC.....	13
114	3.1.3.1 Sektorqualifizierung.....	13
115	3.1.3.2 Sektorzulassung.....	14
116	3.1.4 Kartenpersonalisierer.....	14
117	3.1.5 Zertifikatsnehmer	14
118	3.1.5.1 Karteninhaber (eGK).....	14
119	3.1.5.2 Karteninhaber (HBA, SM-B für medizinische Institutionen oder	
120	Kostenträger)	14
121	3.1.5.3 Karteninhaber (gSMC, SM-B für Gesellschafterorganisationen).....	15
122	3.2 Nachbarsysteme.....	15
123	3.3 Zugriffsprofile.....	16
124	3.4 Sperren und Nachladen von CV-Zertifikaten der Karten- generation 2	17
125	4 Übergreifende Festlegungen	18
126	4.1 Erstellung Ausgabepolicy durch TSP-CVC	18
127	4.2 Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-CVC.....	18
128	4.3 Zulassung	19
129	4.4 Registrierung und Sektorqualifizierung	19
130	4.5 Zusammenspiel Kartenherausgeber, CVC-CA und Kartenpersonalisierer .	19
131	4.6 Mindestanforderungen an eine CVC-CA	22
132	4.6.1 Schutzbedarfsfeststellung.....	22
133	4.6.2 Verfügbarkeit der CVC-CA	23
134	4.6.3 Ausschließlichkeit und Dauer der Schlüsselnutzung	23
135	4.6.4 Verlust der Zulassung	24
136	4.6.5 Sicherheit des Schlüsselpaares.....	24
137	4.6.6 Algorithmen und Schlüssellängen	27
138	4.6.7 Schlüsselversionen.....	28
139	4.6.8 Protokollierung	28
140	4.6.9 Personelle Anforderungen.....	30
141	4.6.10 Betriebliche Anforderungen.....	31
142	4.6.11 Authentizität des öffentlichen Schlüssels der CVC-CA.....	32
143	4.6.12 Synchronisierung mit dem Zeitdienst	32
144	4.7 Beantragung eines CV-Zertifikats für die CVC-CA	32
145	4.8 Unterscheidung produktiver CVC-CA und Test-CVC-CA	35
146	5 Funktionsmerkmale	36
147	5.1 Ausstellung von CV-Kartenzertifikaten durch CVC-CA	36
148	5.1.1 Schnittstelle P_CVC_Provisioning.....	36
149	5.1.1.1 Schnittstellendefinition.....	36
150	5.1.1.2 Umsetzung.....	38
151	5.1.2 Artefakte	39
152	5.1.2.1 Card Holder Reference	39
153	5.1.2.2 Card Holder Authorization Template (CHAT)	39
154	5.1.2.3 Certificate Authority Reference	39
155	5.1.2.4 Datenobjekte eines CV-Zertifikats der Generation 2.....	40

156	5.1.3 Testunterstützung	40
157	6 Anhang – Verzeichnisse	41
158	6.1 Abkürzungen	41
159	6.2 Glossar	42
160	6.3 Abbildungsverzeichnis.....	42
161	6.4 Tabellenverzeichnis	42
162	6.5 Referenzierte Dokumente.....	43
163	6.5.1 Dokumente der gematik.....	43
164	6.5.2 Weitere Dokumente.....	43
165		

ENTWURF

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 oder an einen von ihm benannten Dritten beschrieben.

1.2 Zielgruppe

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

198 1.5 Methodik

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

203 Sie werden im Dokument wie folgt dargestellt:

204 **<AFO-ID> - <Titel der Afo>**

205 Text / Beschreibung

206 [**<=>**]

207

208 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke
209 angeführten Inhalte.

210 1.6 Unterscheidung der Anforderungsadressaten

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

- 215 • Für eGK: Kartenherausgeber und Kartenpersonalisierer
- 216 • Für HBA/SMC-B: Kartenherausgeber oder ein von ihm benannter Dritter (zum
217 Beispiel TSP-CVC)
- 218 • Für Gerätekarten (gSMC-K und -KT): Gerätehersteller (Konnektor-
219 /Kartenterminal-Hersteller) (Gemäß Kapitel 2.7.3.4 aus [gemKPT_PKI_TIP])

220

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 wurden die CV-Zertifikate auf ECC-basierte Kryptographie umgestellt. Eine Cross-Zertifizierung zwischen zwei Zertifizierungsstellen RSA-basierten (G1) und ECC-basierten CVC-PKI (G2) besteht nicht

Die Grundlagen und die Hierarchie der PKI für CV-Zertifikate sind in [gemKPT_PKI_TIP#5] beschrieben. Das zugehörige Vertrauensmodell wird in Kapitel 2.3.6 ebenfalls erläutert. Anforderungen an die Zertifikatsprofile sowie an die Prüfung von CV-Zertifikaten sind in [gemSpec_PKI] in den Kapiteln 6.7 (Zertifikatsprofile) sowie in 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 die Kartengeneration 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 (Hardware-Sicherheitsmodul) 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

262 SMC-B entsprechen. Als Oberbegriff wird die Bezeichnung SM-B bzw. Sicherheitsmodul
263 vom Typ B benutzt. Eine Unterscheidung zwischen SMC-B und HSM-B wird jedoch
264 vorgenommen, wenn sie für die konkrete inhaltliche Betrachtung relevant ist.

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

268

ENTWURF

3 Systemkontext

3.1 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.

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

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 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.

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.

3.1.3.1 Sektorqualifizierung

Falls CV-Rollenzertifikate erzeugt werden sollen, benötigt die CVC-CA hierfür eine Sektorqualifizierung durch die jeweils zuständige Qualifizierende Stelle gemäß [gemSpec_PKI#Tab_PKI_254], welche durch die gematik eingeholt wird.

348 Die Sektorqualifizierung dient als Zustimmung oder Erlaubnis der Qualifizierenden Stelle,
349 dass der Betreiber der CVC-CA autorisiert ist, die genannten Zugriffsprofile in die CV-
350 Rollenzertifikate einzubringen.

351 Für die Erzeugung von CV-Gerätecertifikaten und CV-Zertifikaten mit dem Rollenprofil 0
352 für eGK benötigt die CVC-CA keine Sektorqualifizierung.

353 Grundsätzlich kann jedoch der Kartenherausgeber einen TSP-CVC seiner Wahl
354 beauftragen. Zugelassene Produkttypen TSP-CVC bieten, abgesehen von der ggf.
355 spezifischen Sektorqualifizierung, die gleichen Funktionen (vgl.
356 [gemKPT_Arch_TIP#5.2]).

357 **3.1.3.2 Sektorzulassung**

358 Die Zulassung des Anbieter SMC-B/HBA ist erforderlich für die Erteilung der sektoralen
359 Zulassung (kurz: Sektorzulassung).

360 **A_15170 - Sektorzulassung für zugelassene TSP-CVC**

361 Ein durch die gematik zugelassener Anbieter HBA/SMC-B MUSS zusätzlich ein sektorales
362 Zulassungsverfahren erfolgreich durchlaufen, um HBA/SMC-B der
363 Leistungserbringergorganisation an Endkunden auszugeben. [≤]

364 Festlegungen zu den für die Sektorzulassung vorgesehenen Rollenprofilen trifft der
365 zuständige Sektor (vgl. [gemZul_Prod_CVC#4 – Fussnote 1]).
366

367 **3.1.4 Kartenpersonalisierer**

368 Der Begriff des Kartenpersonalisierers wird in [gemGlossar] definiert.

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

375 **3.1.5 Zertifikatsnehmer**

376 **3.1.5.1 Karteninhaber (eGK)**

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

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

382 **3.1.5.2 Karteninhaber (HBA, SM-B für medizinische Institutionen oder** 383 **Kostenträger)**

384 Ein HBA bzw. eine SM-B für medizinische Institutionen oder Kostenträger enthält ein CV-
385 Rollenzertifikat mit einem Zugriffsprofil ungleich 0. Das genaue Zugriffsprofil ist dabei
386 abhängig von der Berufsgruppe, zu der der Karteninhaber des HBA (Leistungserbringer,
387 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 enthalten zusätzlich zu den CV-Rollenzertifikaten auch je ein CV-Gerätezertifikat. Aus dessen Existenz ergeben sich keine weiteren Pflichten für den Karteninhaber.

3.1.5.3 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.

3.2 Nachbarsysteme

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

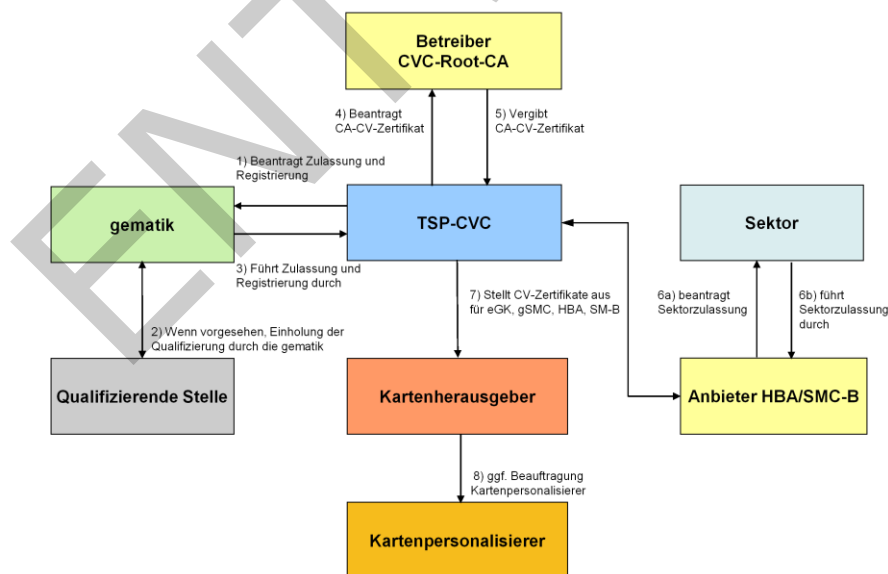


Abbildung 1: Beispielhafte Nachbarsysteme eines TSP-CVC

Die Qualifizierung eines TSP-CVC zur Ausgabe von Rollenzertifikaten für den Zugriff auf medizinische Daten wird durch eine zuständige Qualifizierende Stelle gemäß [gemSpec_PKI#Tab_PKI_254] vergeben und durch die gematik eingeholt (Schritte 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 CHAT.0 (eGK) oder CHAT.8 (SM-B ohne Zugriff auf medizinische Daten).

Für den Prozess der Zulassung und Registrierung (Schritte 1 und 3) 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.

Die sektorale Zulassung eines durch die gematik zugelassenen Anbieters HBA/SMC-B wird durch einen zuständigen Sektor erteilt (Schritte 6a und 6b).

Für die Erzeugung der CV-Zertifikate des TSP-CVC bestehen technische und organisatorische Schnittstellen zur CVC-Root-CA (Schritte 4 und 5) 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 gegebenenfalls durch den Kartenpersonalisierer an einen von ihm benannten Dritten übertragen (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#6.7.3.5] enthalten.

Mit seiner Zulassung erhält ein TSP-CVC das grundsätzliche Recht, CV-Zertifikate zu erzeugen.

Für spezifische Zugriffsprofile (z. B. das Rollenprofil 2) ist nicht nur eine Registrierung einer CVC-CA, sondern auch eine Sektorqualifizierung erforderlich. Die Zulassung und Registrierung erfolgt durch die gematik, eine Qualifizierung wird durch die zuständige Qualifizierende Stelle gemäß [gemSpec_PKI#Tab_PKI_254] ausgesprochen und durch die gematik eingeholt. Die Bezeichnung „spezifische Zugriffsprofile“ wird im Folgenden verwendet, sofern die Ausgabe von CV-Zertifikaten mit solchen Zugriffsprofilen einer Qualifizierung bedarf.

Unabhängig von der technischen Umsetzung in CV-Zertifikaten wird in diesem Dokument (anstelle CHA.X für die Rollen gemäß der Bezeichnung für die Kartengeneration 1) CHAT.X jeweils für die Zugriffsprofile verwendet (z.B. Zugriffsprofil 1 (CHAT.1) für CV-Rollen-Zertifikat oder Zugriffsprofil 51 (CHAT.51) für ein G2-CV-Geräte-Zertifikat). Die Umsetzung für die Kartengeneration 2 erfolgt dann gemäß den Vorgaben zum Parameter Certificate Holder Authorisation Template (CHAT/Flaglist) in [gemSpec_PKI#6.7.3.5].

456 **3.4 Sperren und Nachladen von CV-Zertifikaten der Karten-**
457 **generation 2**

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

ENTWURF

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:

1. Identifizierung von Anforderungen an den Betrieb,
2. Angaben zu organisatorischen und technischen Sicherheitsanforderungen,
3. Identifizierung von Antragstellern, die CV-Zertifikate beziehen möchten,
4. Festlegungen von Namensregelungen zur CVC-CA,
5. Identifizierung von Profilen, für die CV-Zertifikate ausgestellt werden,
6. Angaben zu Zertifikatsprofilen,
7. 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.

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.

4.3 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.

4.4 Registrierung und Sektorqualifizierung

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. Mit einer erfolgreichen Registrierung, ist die CVC-CA berechtigt, CV-Zertifikate mit den festgelegten Profilen zu erzeugen.

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.

Auf Anfrage der gematik bestätigt die zuständige Qualifizierende Stelle gemäß [gemSpec_PKI#Tab_PKI_254] gegenüber der Registrierungsstelle der gematik, dass die Sektorqualifizierung für die CVC-CA erteilt wird. Wie die Bestätigung durchzuführen ist, wird je Sektor mit der gematik vereinbart. Der TSP-CVC darf kein CV-Zertifikat mit einem bestimmten Zugriffsprofil erzeugen, ohne die zugehörige Sektorqualifizierung erhalten zu haben.

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 mit solchen Zugriffsprofilen erzeugt werden, die im Rahmen des Registrierungsprozesses durch die jeweils verantwortliche Qualifizierende Stelle freigegeben wurden. Abweichungen hiervon führen zu einem unverzüglichen Widerruf der Registrierung.

[<=]

Eine Zuordnung, welche Qualifizierende Stelle verantwortlich für die jeweilige Qualifizierung ist, ist in [gemSpec_PKI#6.3.1, Tab_PKI_254] festgelegt.

4.5 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 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

1. FIPS 140-2 Level 3,
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder
3. 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

584 anderen HSM gelöscht wird.

585 [\leq]

586 **TIP1-A_2583 - Zuordnung des privaten Schlüssels zu Identitäten**

587 Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS sicherstellen, dass ein privater
588 Schlüssel nicht zwei verschiedenen Identitäten zugeordnet wird.

589 [\leq]

590 **TIP1-A_2584 - Schlüsselpaare und CV-Zertifikate**

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

595 [\leq]

596 *Hinweis: Eine eGK enthält als eigenes CV-Zertifikat nur ein CV-Rollen-Zertifikat*
597 *(C.eGK.AUT_CVC) mit dem Zugriffsprofil CHAT.0.*

598 Eine gSMC-KT enthält als eigenes CV-Zertifikat nur ein CV-Geräte-Zertifikat
599 (C.SMC.AUTD_RPS_CVC) mit dem Zugriffsprofil CHAT.54.

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

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

606 [\leq]

607 **TIP1-A_2586 - Personalisierung von CV-Zertifikaten für ein Sicherheitsmodul**
608 **vom Typ B**

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

614 [\leq]

615 **TIP1-A_2587 - Personalisierung von CV-Zertifikaten für eine eGK**

616 Bei der Personalisierung einer eGK MUSS der Herausgabeverantwortliche gemäß Kapitel
617 1.6 sicherstellen, dass das einzubringende CV-Zertifikat genau das Zugriffsprofil 0
618 enthält.

619 [\leq]

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

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

623 Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS vor der Verwendung des
624 öffentlichen Schlüssels der CVC-Root-CA die Authentizität dieses Schlüssels sicherstellen.
625 Bei der Personalisierung einer Chipkarte MUSS der Herausgabeverantwortliche gemäß
626 Kapitel 1.6 sicherstellen, dass der CVC-Root-Schlüssel auf der Karte aufgebracht ist, der
627 zur Prüfung des personalisierten CVC-SubCA-Zertifikates benötigt wird. Hinweis: Falls die
628 initialisierte Chipkarte den erforderlichen CVC-Root-Schlüssel nicht enthält, so ist es
629 möglich, diesen durch ein oder mehrere CVC-Root-Cross-Zertifikate aufzubringen.
630 Dabei MUSS der Herausgabeverantwortliche oder ein von ihm benannter Dritter
631 durchgängig das Vier-Augen-Prinzip umsetzen.

632 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.

[<=]

A_16178 - Bezug des CV-Zertifikats mit dem Zugriffsprofil Null für SM-B KTR-AdV

Ein zugelassener TSP-CVC SMC-B KANN mit seiner registrierten CVC-CA gemäß [gemSpec_PKI#Tab_PKI_919] CV-Zertifikate mit dem Zugriffsprofil CHAT.0 für KTR-AdV ausstellen.[<=]

Für die Etablierung eines Trusted Channel zu einer eGK mittels einer Card-to-Card-Authentisierung benötigt die KTR-AdV zusätzlich ein CV-Zertifikat mit dem Zugriffsprofil CHAT.0. Ein zugelassener TSP-CVC kann benötigte CV-Zertifikate mit dem Rollenprofil CHAT.0 für eine KTR-AdV bereitstellen.

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, eines Sicherheitsmoduls vom Typ B bzw. der KTR-AdV 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 bzw. der KTR-AdV,
 (i) Zulassungsdokumente,
 (j) Registrierungsdokumente,
 (k) Authentisierungsinformationen zur Authentisierung von Akteuren bzw. Rollen,
 (l) Protokolldaten und
 (m) 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.

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_2599-01TIP1-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:

1. physisches Löschen des privaten Schlüssels innerhalb des HSM,
2. 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

- 766 1. der private Schlüssel für die Erzeugung von Zertifikaten nicht auslesbar in einem
767 Hardware-Sicherheitsmodul (HSM) gespeichert wird und
- 768 2. nach Verwendung des privaten Schlüssels keine Artefakte der Bearbeitung im
769 System hinterlassen werden, die eine Kompromittierung des Schlüssels
770 ermöglichen oder erleichtern.

771 [**<=**]

772 **TIP1-A_2609 - Einsatz einer Chipkarte als HSM**

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

774 [**<=**]

775 **TIP1-A_4223 - Ordnungsgemäße Sicherung des privaten Schlüssels der CVC-CA**

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

780 [**<=**]

781 **TIP1-A_4224 - Verwendung von privaten Schlüsseln einer CVC-CA**

782 Der TSP-CVC MUSS gewährleisten, dass

- 783 1. alle kryptographischen Berechnungen mit einem privaten Schlüssel einer CVC-CA
784 intern in einem Hardware-Sicherheitsmodul (HSM) durchgeführt werden und
- 785 2. private Schlüssel der CVC-CA nicht im Klartext aus dem HSM exportiert werden
786 können.

787 [**<=**]

788 **TIP1-A_2610 - Möglichkeit zum Klonen eines HSM**

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

793 [**<=**]

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

795 **TIP1-A_2611 - Berücksichtigung des Klonens im Sicherheitskonzept**

796 Der TSP-CVC MUSS den Vorgang des Klonens (ggf. auch abgebildet über Schlüsselbackup
797 und -restore) im Sicherheitskonzept gesondert beschreiben.

798 Dabei MÜSSEN insbesondere die Maßnahmen für die Gewährleistung der Sicherheit des
799 privaten Schlüssels als auch die (technischen und/oder organisatorischen) Maßnahmen
800 für die Verhinderung des unautorisierten Erstellens von Klonen beschrieben werden.

801 [**<=**]

802 **TIP1-A_2612 - Anwendung des Vier-Augen-Prinzips beim Klonen eines HSMs**

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

806 [**<=**]

807 **TIP1-A_2613 - Protokollierung beim Klonen eines HSMs**

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

809 [**<=**]

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

1. FIPS 140-2 Level 3,
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder
3. 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

1. zur Generierung eines neuen Schlüsselpaares,
2. zur Aktivierung eines Schlüsselpaares,
3. zum kryptographisch abgesicherten Import und Export eines privaten Schlüssels,
4. zum (physikalischen) Löschen eines Schlüsselpaares,
5. zur m-von-n-Aktivierung und
6. 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 sensibler Schlüssel

Der TSP-CVC MUSS sicherstellen, dass eine Weitergabe geheimer und privater Schlüssel an andere Organisationen sowie an nicht berechnigte 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

1. 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,
2. für jede Betriebsumgebung ein separates Schlüssel-Backup der CVC-CA nach den vom HSM-Hersteller vorgegebenen Backup-Verfahren sicher erstellen und sicher verwahren,
3. 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.

[<=]

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.

899 Vorgaben zur Migration von Algorithmen und Schlüssellängen und dabei zu beachtender
900 Übergangsfristen sind in [gemSpec_Krypt#3.14] definiert.

901 4.6.7 Schlüsselversionen

902 CVC-CAs der zweiten Ebene setzen für das Ausstellen von CV-Zertifikaten ein
903 Schlüsselpaar ein, dass eine gegebene feste Schlüssellänge hat. Ebenso wird das
904 Schlüsselpaar nur mit einem bestimmten kryptographischen Algorithmus genutzt.
905 Aufgrund fortschreitender Erkenntnisse bezüglich der Sicherheit bestimmter
906 Schlüssellängen bzw. Algorithmen werden nach gewissen zeitlichen Abständen die
907 Nutzung eines neuen (längeren) Schlüsselpaares und ggf. auch die Nutzung neuer
908 kryptographischer Algorithmen für die CVC-CAs der zweiten Ebene notwendig. Ein
909 Wechsel zu einem neuen Schlüsselpaar mit einer größeren Schlüssellänge (und ggf. zu
910 einem neuen Algorithmus) wird als Generationswechsel bezeichnet.

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

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

919 **TIP1-A_2626 - Berücksichtigung von Notfallmaßnahmen im Sicherheitskonzept**
920 Eine Abschätzung der Auswirkungen einer Kompromittierung eines Schlüsselpaares sowie
921 die daraus folgenden Notfallprozesse MÜSSEN durch den TSP-CVC in einer Risikoanalyse
922 und Notfallplanung in seinem Sicherheitskonzept behandelt werden.
923 [\leq]

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

927 **TIP1-A_2627 - Wechsel der Schlüsselversion bei der CVC-CA**
928 Im Falle eines Wechsels der Schlüsselversion MUSS der TSP-CVC den neuen öffentlichen
929 Schlüssel einer CVC-CA durch die CVC-Root-CA zertifizieren lassen. Bei allen im
930 Folgenden durch die CVC-CA zu erzeugenden CV-Zertifikate MUSS die CVC-CA ihr neues
931 Schlüsselpaar verwenden. Entsprechend MUSS bei der Kartenproduktion das neue CV-
932 Zertifikat der CVC-CA in die zugehörigen Karten eingebracht werden.
933 [\leq]

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

938 4.6.8 Protokollierung

939 **TIP1-A_2628 - Protokollierung durch den TSP-CVC - Ereignisse**
940 Die Arbeit des TSP-CVC MUSS revisionssicher protokolliert werden. Mindestens die
941 folgenden Ereignisse MÜSSEN durch den TSP-CVC protokolliert werden:

- 942 1. Generierung eines neuen Schlüsselpaares im HSM,
- 943 2. Löschung eines privaten Schlüssels im HSM,

- 944 3. Export des privaten Schlüssels,
- 945 4. Import des privaten Schlüssels,
- 946 5. Sperrung der Zugriffe auf einen privaten Schlüssel im HSM,
- 947 6. Erzeugen eines CV-Zertifikats mit einem Profil ungleich 0 (CV-Zertifikat für einen
- 948 HBA, ein Sicherheitsmodul vom Typ B oder ein gerätebezogenes
- 949 Sicherheitsmodul),
- 950 7. Erzeugen einer Menge von CV-Zertifikaten mit Profil 0 (CV-Zertifikat für eine eGK
- 951 oder die KTR-AdV).

952 [**<=**]

953 **TIP1-A_2691 - Protokollierung durch den TSP-CVC - Werte**

954 Bei der Protokollierung MÜSSEN durch den TSP-CVC die folgenden Werte protokolliert

955 werden:

- 956 1. Datum und Uhrzeit,
- 957 2. Typ des Ereignisses,
- 958 3. Namen der beiden Mitarbeiter des TSP-CVC, die das HSM frei geschaltet haben.

959 [**<=**]

960 **TIP1-A_2629 - Protokollierung durch den TSP-CVC – Profil ungleich 0**

961 Bei dem Erzeugen eines CV-Zertifikates mit einem Profil ungleich 0 MÜSSEN durch den

962 TSP-CVC zusätzlich die folgenden Werte protokolliert werden:

- 963 1. Name des zuständigen Kartenherausgebers,
- 964 2. Inhalt der Felder CHR und CHAT bei Kartengeneration 2,
- 965 3. das erstellte CV-Zertifikat selber.

966 [**<=**]

967 **TIP1-A_2692 - Protokollierung durch den TSP-CVC – Profil gleich 0**

968 Der TSP-CVC MUSS bei dem Erzeugen von CV-Zertifikaten mit einem Profil gleich 0 die

969 folgenden Werte protokollieren:

- 970 1. Name des zuständigen Kartenherausgebers,
- 971 2. Inhalt der Felder CHR und CHAT bei Kartengeneration 2,
- 972 3. das erstellte CV-Zertifikat selber,
- 973 4. Anzahl der erzeugten CV-Zertifikate.

974 [**<=**]

975 **TIP1-A_2630 - Protokollierung pro Bestellung/Produktionslauf (Profil gleich 0)**

976 Die Protokollierung durch den TSP-CVC bei dem Erzeugen von CV-Zertifikaten mit Profil

977 gleich 0 SOLL pro Bestellung/Produktionslauf geschehen.

978 [**<=**]

979 **TIP1-A_2631 - Nachvollziehbarkeit bei Produktion mit Profil 0**

980 Der TSP-CVC MUSS sicherstellen, dass dabei nachträglich anhand der Protokolle

981 nachvollzogen werden kann, wann wie viele CV-Zertifikate mit einem Profil gleich 0 für

982 wen erzeugt wurden.

983 [**<=**]

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:

1. Leiter CVC-CA,
2. Sicherheitsbeauftragter CVC-CA,
3. Antragsteller CVC-CA-Zertifikat,
4. Zertifizierer,
5. 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_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:

1. Der Zugang zu diesem Bereich ist nur autorisierten Mitarbeitern möglich.
2. Beim Zugang muss der Mitarbeiter eindeutig identifiziert werden.
3. Der Zugang zu diesem Bereich wird protokolliert.
4. Alle Zugänge sind in geeigneter Weise gegen Einbruch gesichert.
5. Ist kein berechtigter Mitarbeiter anwesend, wird der Bereich alarmüberwacht.
6. 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:

1. Umsetzung einer Benutzerauthentisierung, die mindestens dem Sicherheitsniveau eines Logins mit Username und Passwort entspricht,
2. Umsetzung einer Zugriffskontrolle,
3. Sichere Administration und Konfiguration von Komponenten,
4. Maßnahmen zur Systemhärtung,

- 1070 5. Zeitnahes Einspielen von Updates, insbesondere von Sicherheitsupdates,
1071 6. Einsatz aktueller Virenschutzprogramme.
1072 [\leq]

1073 **4.6.11 Authentizität des öffentlichen Schlüssels der CVC-CA**

1074 Der Anbieter der CVC-Root-CA setzt für den Prozess der Ausstellung eines Zertifikats
1075 durchgängig in und zwischen allen Arbeitsschritten, d.h. vom Eingang des
1076 Zertifikatsausstellungsantrags bis hin zur Übergabe des Zertifikats an den Antragssteller,
1077 das Vier-Augen-Prinzip um.

1078 **TIP1-A_2648 - Vier-Augen-Prinzip bei Beantragung des CVC-CA-Zertifikats**

1079 Der TSP-CVC MUSS für den Gesamtprozess der Beantragung und des Erhalts eines CVC-
1080 CA-Zertifikats bei einer CVC-Root-CA das Vier-Augen-Prinzip umsetzen.
1081 [\leq]

1082 Dies kann bspw. dadurch erfolgen, dass den Zertifikatsausstellungsantrag zwei
1083 Mitarbeiter der CVC-CA auf Korrektheit direkt vor der Abgabe an den Anbieter der CVC-
1084 Root-CA im Vier-Augen-Prinzip prüfen und diese Prüfung dokumentieren.

1085 **TIP1-A_2649 - Konsistenzprüfung des ausgestellten CVC-CA-Zertifikats**

1086 Bei erfolgreicher Ausstellung des beantragten Zertifikats MÜSSEN mindestens zwei
1087 Mitarbeiter des TSP-CVC das von der CVC-Root-CA übergebene Zertifikat auf Konsistenz
1088 bezüglich des Zertifikatsausstellungsantrags prüfen sowie das Prüfergebnis
1089 dokumentieren und revisionssicher aufbewahren.
1090 [\leq]

1091 **TIP1-A_2650 - Behandlung negativer Prüfergebnisse im Sicherheitskonzept**

1092 Für fehlgeschlagene Prüfergebnisse MUSS der TSP-CVC Notfallmaßnahmen in seinem
1093 Sicherheitskonzept definieren und diese im Eintrittsfalle einleiten.
1094 [\leq]

1095 Das bei Ausstellung eines Zertifikats durch die CVC-Root-CA angewandte Vier-Augen-
1096 Prinzip muss mit dem Vier-Augen-Prinzip der Beantragung und des Erhalts des Zertifikats
1097 durch den TSP-CVC so ineinandergreifen, dass die Durchgängigkeit des Vier-Augen-
1098 Prinzip garantiert ist.

1099 **4.6.12 Synchronisierung mit dem Zeitdienst**

1100 **TIP1-A_2695 - Verfahren zur Zeitsynchronisierung**

1101 Ein TSP-CVC MUSS ein Verfahren zur Zeitsynchronisierung einsetzen, das eine maximale
1102 Abweichung von einer Sekunde gegenüber der gesetzlichen Zeit der Physikalisch-
1103 Technischen Bundesanstalt (PTB) gewährleistet.
1104 [\leq]

1105 **4.7 Beantragung eines CV-Zertifikats für die CVC-CA**

1106 Nach erfolgreicher Zulassung und Registrierung kann ein TSP-CVC für einen öffentlichen
1107 Schlüssel einer CVC-CA ein CVC-CA-Zertifikat bei der CVC-Root-CA beantragen. Die
1108 Festlegungen zur Nutzung der organisatorischen Schnittstelle
1109 P_Sub_CA_Certification_CVC durch den TSP-CVC werden im Folgenden beschrieben.
1110 Die Beantragung geschieht in zwei Schritten:

- 1111 • Der TSP-CVC stellt einen schriftlichen Antrag bei der CVC-Root-CA. Als
- 1112 Antwort wird ihm ein Termin mitgeteilt, an dem der Mitarbeiter des TSP-CVC
- 1113 das CVC-CA-Zertifikat persönlich bei der CVC-Root-CA abholen kann.
- 1114 • An dem genannten Termin überbringt ein Mitarbeiter des TSP-CVC den CVC-
- 1115 PKCS#10-Request persönlich an die CVC-Root-CA. Nach Bearbeitung erhält er
- 1116 das neue CVC-CA-Zertifikat.

1117 **TIP1-A_2654 - Antrag für ein CVC-CA-Zertifikat bei der CVC-Root-CA**

1118 Der TSP-CVC MUSS ein neues CVC-CA-Zertifikat für ihr Schlüsselpaar schriftlich bei der

1119 CVC-Root-CA beantragen. Hierzu MUSS der TSP-CVC die von der CVC-Root-CA zur

1120 Verfügung gestellte Schnittstelle P_Sub_CA_Certification_CVC nutzen.

1121 [\leq]

1122 **TIP1-A_4228 - Angaben in der Beantragung eines CVC-CA-Zertifikats**

1123 Mit der Beantragung eines CVC-CA-Zertifikats bei der CVC-Root-CA MUSS der TSP-CVC

1124 die folgenden Angaben bereitstellen:

- 1125 1. Name und Anschrift der CVC-CA,
- 1126 2. CA-Name im Zertifikat (5 ASCII-Zeichen),
- 1127 3. Typ des gewünschten Zertifikats (produktive CVC-CA oder Test-CVC-CA),
- 1128 4. Name und Vorname einer Kontaktperson,
- 1129 5. Fingerprint über den öffentlichen Schlüssel, für den das CVC-CA-Zertifikat erzeugt
- 1130 werden soll,
- 1131 6. Unterschriften zweier hierfür berechtigter Mitarbeiter des TSP-CVC.

1132 [\leq]

1133 **TIP1-A_2655 - Konsistenz des CA-Namens**

1134 Der TSP-CVC MUSS sicherstellen, dass die Angaben zu "Name und Anschrift der CVC-CA"

1135 sowie "CA-Name im Zertifikat" identisch sind zu seinen Angaben in der Registrierung

1136 bzw. der zugehörigen letzten Änderungsmitteilung.

1137 [\leq]

1138 **TIP1-A_2656 - Beantragung und Rollen**

1139 Der TSP-CVC MUSS bei der Beantragung eines CVC-CA-Zertifikats Kontaktpersonen

1140 angeben, die im Rahmen der Zulassung (oder einer Änderung) angegeben wurden und

1141 eine der Rollen "Leiter CA", "Sicherheitsbeauftragter" bzw. "Antragsteller CVC-CA-

1142 Zertifikat" inne haben. Der TSP-CVC MUSS sicherstellen, dass eine der Unterschriften von

1143 einem Mitarbeiter stammt, dem die Rolle "Leiter CVC-CA" zugewiesen wurde. Weiterhin

1144 MUSS der TSP-CVC sicherstellen, dass die zweite Unterschrift von einem weiteren bei der

1145 Zulassung bzw. einer Änderungsmitteilung genannten Mitarbeiter

1146 ("Sicherheitsbeauftragter" bzw. "Antragsteller CVC-CA-Zertifikat") stammt.

1147 [\leq]

1148 Nach Eingang eines schriftlichen Antrags prüft der Anbieter der CVC-Root-CA den

1149 eingegangenen Antrag. Grundlage für die Überprüfungen ist die aktuelle Liste mit den

1150 zugelassenen TSP-CVCs und registrierten CVC-CAs, die die gematik dem Anbieter der

1151 CVC-Root-CA regelmäßig zur Verfügung stellt.

1152 Haben alle Überprüfungen ein positives Ergebnis, bestätigt der Anbieter der CVC-Root-CA

1153 schriftlich dem TSP-CVC den Antrag und teilt dabei den Termin mit, an dem das

1154 eigentliche Zertifikat erzeugt werden soll.

1155 Die CVC-Root-CA wird nur dann ein CVC-CA-Zertifikat für die CVC-CA ausstellen, falls der

1156 CVC-PKCS#10-Request persönlich durch einen hierfür vorher genannten Mitarbeiter

1157 überbracht wird.

1158 Hat eine der Überprüfungen ein negatives Ergebnis, wird der Antrag durch den Anbieter
1159 der CVC-Root-CA abgelehnt. Der TSP-CVC wird entsprechend schriftlich informiert.

1160 **TIP1-A_2657 - Korrektheit der Angaben**

1161 Der TSP-CVC MUSS die Korrektheit der Werte in seinem Request für ein CV-Zertifikat
1162 sicherstellen.

1163 [\leq]

1164 Der Anbieter der CVC-Root-CA übernimmt die angegebenen Werte in das CV-Zertifikat
1165 der CVC-CA.

1166 **TIP1-A_2658 - Nutzung der Schnittstelle zur Beantragung eines CVC-CA-**
1167 **Zertifikats**

1168 Zur Nutzung der Schnittstelle bzw. zur Durchführung der Beantragung eines CVC-CA-
1169 Zertifikats MÜSSEN durch die CVC-CA die folgenden Schritte durchgeführt werden:

- 1170 1. Das Formular zur Beantragung eines CVC-CA-Zertifikats wird von den Web-Seiten
1171 des Anbieters der CVC-Root-CA heruntergeladen, ausgefüllt und (handschriftlich)
1172 unterschrieben. Dieses Formular wird an den Anbieter der CVC-Root-CA
1173 gesendet.
- 1174 2. Nach positiver Prüfung des Antrags durch den Anbieter der CVC-Root-CA erhält
1175 der TSP-CVC den Termin mitgeteilt, an dem das CVC-CA-Zertifikat erzeugt werden
1176 soll.
- 1177 3. Falls bisher noch nicht geschehen, MUSS die Schlüsselgenerierung für die CVC-CA
1178 durch den TSP-CVC vorgenommen werden.
- 1179 4. Der TSP-CVC erzeugt für das Schlüsselpaar einen Request.
- 1180 5. Der Request MUSS gesichert durch einen dazu berechtigten Mitarbeiter des TSP-
1181 CVC persönlich an den vereinbarten Termin an die CVC-Root-CA überbracht
1182 werden.
- 1183 6. Nach Erzeugung des CVC-CA-Zertifikats durch die CVC-Root-CA wird das Zertifikat
1184 unter Anwendung des Vier-Augen-Prinzips in die Systeme des TSP-CVC
1185 eingebracht.
- 1186 7. Die (nicht) erfolgreiche Durchführung des Prozesses MUSS einschließlich der
1187 Beantragung durch den TSP-CVC dokumentiert und revisionssicher aufbewahrt
1188 werden.

1189 [\leq]

1190 **TIP1-A_2659 - Name der CA**

1191 Jede produktive und jede Test-CVC-CA MUSS einen innerhalb einer Kartengeneration
1192 eindeutigen CA-Namen (5 ASCII-Zeichen) verwenden. Dabei gilt:

- 1193 1. Bei einer in Deutschland betriebenen CVC-CA MUSS der CA-Name bei der hierfür
1194 durch den DIN beauftragten Registrierungsstelle (Fraunhofer Gesellschaft SIT)
1195 registriert sein.
- 1196 2. Bei einer außerhalb Deutschlands betriebenen CVC-CA MUSS der CA-Name bei der
1197 jeweils zuständigen nationalen Registrierungsstelle registriert sein.

1198 [\leq]

1199 Bisherige Kennungen und Antragsformular stehen unter www.sit.fraunhofer.de. Diese
1200 CA-Namen beginnen mit den zwei Zeichen DE.

1201 **TIP1-A_2660 - CA-Namen bei Betrieb mehrerer CVC-CAs**

1202 Hat ein TSP-CVC verschiedene CVC-CAs, mit denen er CV-Zertifikate für verschiedene
1203 Kartengenerationen erzeugt, so KÖNNEN diese CVC-CAs den gleichen CA-Namen haben.
1204 [\leq]

1205 **TIP1-A_3029 - Name einer Test-CVC-CA**

1206 Der TSP-CVC MUSS sicherstellen, dass die CA-Namen für Test-CVC-CA und der
1207 produktiven CVC-CA unterschiedlich sind sowie der CA-Name für die Test-CVC-CA ein X
1208 enthält.
1209 [\leq]

1210 **TIP1-A_2696 - Sicherstellung der Zuordnung von CV-Zertifikaten bei mehreren**
1211 **CVC-CAs mit gleichem Namen**

1212 Sofern ein TSP-CVC verschiedene CVC-CAs mit gleichem CA-Namen betreibt, MUSS er
1213 über die Belegung des Feldes Certificate Authority Reference (CAR) sicherstellen, dass
1214 die erzeugten CV-Zertifikate eindeutig der ausgebenden CVC-CA zugeordnet werden
1215 können.
1216 [\leq]

1217 *Hinweis: Die technischen Details der Schnittstelle P_Sub_CA_Certification_CVC sind in*
1218 *gemSpec_CVC_Root im Kapitel 6.1 beschrieben. Zur Vermeidung von Redundanzen wird*
1219 *daher der nachfolgende Block entfernt.*

1220 **4.8 Unterscheidung produktiver CVC-CA und Test-CVC-CA**

1221 Bei der PKI für CV-Zertifikate wird zwischen einer Produktiv-PKI und einer Test-PKI
1222 unterschieden.

1223 **TIP1-A_3030 - Betrieb von Test-CVC-CAs**

1224 Jeder TSP-CVC der zweiten Ebene MUSS neben einer produktiven CVC-CA ebenfalls eine
1225 Test-CVC-CA betreiben.
1226 [\leq]

1228 **TIP1-A_3031 - Registrierung einer Test-CVC-CA**

1229 Der TSP-CVC MUSS eine Test-CVC-CA bei der gematik registrieren.
1230 [\leq]

1231 Die Qualifizierung einer Test-CVC-CA, die zur Ausgabe von Test-CV-Zertifikaten mit
1232 Rollenprofil ungleich 0 und 8 vorgesehen ist, ist nicht erforderlich.

1233 Die Prozesse zur Beantragung eines „Test-CVC-CA-Zertifikats“ sowie zur Ausgabe von
1234 „Test-CV-Zertifikaten“ sind für die produktive CVC-CA und für die Test-CVC-CA identisch.

1235

5 Funktionsmerkmale

1236 Ein Antrag für ein CV-Zertifikat für eine Chipkarte (eGK, HBA, SM-B, gSMC) darf nur
1237 durch den Herausgeber dieser Chipkarte oder. durch einen von diesem benannten Dritten
1238 gestellt werden. Der Antrag muss bei dem TSP-CVC gestellt werden. Details dieses
1239 Vorgangs müssen zwischen Kartenherausgeber, CVC-CA und
1240 Kartenpersonalisierergeregelt werden (sofern der Kartenherausgeber diese Funktionen
1241 nicht selbst ausführt). Grundlegende Anforderungen hierzu siehe Abschnitt 4.5.

1242 Bei der Generierung eines CV-Zertifikats müssen die Anforderungen aus Kapitel 4
1243 eingehalten werden.

1244 Nach der Generierung muss das CV-Zertifikat in die zugehörige Chipkarte eingebracht
1245 werden (Staging). Die hierfür notwendigen Prozesse müssen bilateral zwischen der CVC-
1246 CA und dem Kartenpersonalisierer festgelegt werden. Grundlegende Anforderungen
1247 hierzu siehe Abschnitt 4.5.

1248 CV-Zertifikate können gemäß [gemKPT_PKI_TIP#5.5] nicht gesperrt werden. Muss die
1249 Einsetzbarkeit eines CV-Zertifikats bei Vorliegen eines schwerwiegenden Problems
1250 beendet werden, kann dies nur durch Einziehen und Zerstören der zugehörigen Chipkarte
1251 erreicht werden.

1252 5.1 Ausstellung von CV-Kartenzertifikaten durch CVC-CA

1253 **TIP1-A_2665 - Berechtigung des Antragstellers für CV-Zertifikate**

1254 Der TSP CVC MUSS den Herausgabeverantwortlichen gemäß Kapitel 1.6 als berechtigte
1255 Antragsteller von CV-Zertifikaten authentifizieren. D.h. die CVC-CA erzeugt nur dann die
1256 beantragten CV-Zertifikate, sofern die Berechtigung des Antragstellers erfolgreich
1257 verifiziert werden konnte.

1258 [\leq]

1259 **TIP1-A_2666 - Schriftliche Beantragung von CV-Zertifikaten durch einen** 1260 **Kartenherausgeber**

1261 Die Beantragung von CV-Zertifikaten durch den Herausgabeverantwortlichen gemäß
1262 Kapitel 1.6 bei dem TSP-CVC MUSS bei dem TSP CVC dokumentiert werden.

1263 [\leq]

1264 Entsprechende Informationen werden auf den Web-Seiten der gematik zur Verfügung
1265 gestellt und regelmäßig aktualisiert.

1266 5.1.1 Schnittstelle P_CVC_Provisioning

1267 5.1.1.1 Schnittstellendefinition

1268 **TIP1-A_2668 - Zur Verfügung gestellte Eingangsdaten zur Erzeugung von CV-** 1269 **Zertifikaten**

1270 Der Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS pro CV-Zertifikat mindestens
1271 die folgenden Eingangsdaten für CV-Zertifikate zur Verfügung stellen:

- 1272 1. Öffentlicher Schlüssel
- 1273 2. Card Holder Referenz, CHR, bestehend aus 'xx xx' || ICCSN der Chipkarte (der
1274 Wert 'xx xx' wird durch die einzelnen konkreten Chipkartenspezifikationen der
1275 gematik festgelegt und in Tabelle gemSpec_PKI#TAB_PKI_258 dargestellt.)

1276 3. Certificate Holder Authorisation Template (CHAT), bestehend aus entsprechender
1277 Flagliste für CV-Zertifikate der Kartengeneration 2 (vgl.
1278 [gemSpec_PKI#Tab_PKI_918])

1279 4. Typ des CV-Zertifikats (Test oder produktiv).

1280 [\leq]

1281 **TIP1-A_2669 - Ausgangsdaten der CV-Zertifikatserzeugung, die durch die CVC-**
1282 **CA zur Verfügung gestellt werden**

1283 Durch die CVC-CA MÜSSEN für jedes erzeugte CV-Zertifikat mindestens die folgenden
1284 Daten an den Herausgabeverantwortlichen gemäß Kapitel 1.6 zurückgegeben werden:

1285 1. Erzeugtes CV-Zertifikat,

1286 2. CV-Zertifikat der CVC-CA.

1287 [\leq]

1288 Die CVC-CA muss ihr aktuelles CVC-CA-Zertifikat den Kartenpersonalisierern zur

1289 **TIP1-A_2671 - Anforderungen an die Datenintegrität und -authentizität**

1290 Für den Datenaustausch mit dem Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS
1291 der TSP-CVC einen Mechanismus zur Sicherung der Datenintegrität und -authentizität zur
1292 Verfügung stellen.

1293 [\leq]

1294 Zur Sicherung der Datenintegrität und -authentizität können Mechanismen auf Basis
1295 symmetrischer oder asymmetrischer Kryptographie eingesetzt werden. Hierbei sind die
1296 Anforderungen zur Verwendung kryptographischer Algorithmen in der
1297 Telematikinfrastruktur zu berücksichtigen [gemSpec_Krypt].

1298 **TIP1-A_2672 - Anforderungen an die Vertraulichkeit**

1299 Für den Datenaustausch mit dem Herausgabeverantwortliche gemäß Kapitel 1.6 MUSS
1300 der TSP-CVC einen Mechanismus zur Verschlüsselung der Daten zur Verfügung stellen.

1301 [\leq]

1302 Zur Wahrung der Vertraulichkeit können Mechanismen auf Basis symmetrischer oder
1303 asymmetrischer Kryptographie eingesetzt werden. Hierbei sind die Anforderungen zur
1304 Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur zu
1305 berücksichtigen [gemSpec_Krypt].

1306

1307 **A_17233 - Personalisierung von HSMs der KTR-AdV (CVC)**

1308 Ein TSP-CVC SMC-B MUSS, wenn er mit dem Betreiber einer KTR-AdV einen sicheren
1309 Prozess zur Personalisierung von HSMs definiert und etabliert, alle in [gemSpec_KTR-
1310 AdV#TAB_ADV_385] genannten Aspekte berücksichtigen. Dies betrifft CV-Zertifikate mit
1311 den RollenZugriffsprofilen CHAT.0 und CHAT.1 gemäß
1312 [gemSpec_PKI#TAB_PKI_254]. [\leq]

1313

1314 **A_17642 - Personalisierung von HSMs der KTR-Consumer (CVC)**

1315 Ein TSP-CVC SMC-B MUSS, wenn er mit dem Betreiber eines KTR-Consumer einen
1316 sicheren Prozess zur Personalisierung von HSMs definiert und etabliert, alle in
1317 [gemSpec_Basis_KTR_Consumer#Tab_Personalisierung_HSM] genannten Aspekte
1318 berücksichtigen. Dies betrifft CV-Zertifikate mit dem RollenZugriffsprofil CHAT.8 gemäß
1319 [gemSpec_PKI#TAB_PKI_254]. [\leq]

1320

1321 Falls für einen Prozess zur HSM-Personalisierung nur eine geringe Anzahl an Instanzen
1322 erwartet wird, kann es sinnvoll sein, Teile dieses Prozesses rein organisatorisch
1323 umzusetzen. Anstelle einer technischen Schnittstelle kann dann ein papierbasiertes
1324 Verfahren eingesetzt werden.
1325

1326 5.1.1.2 Umsetzung

1327 Der TSP-CVC nimmt die Eingangsdaten des Herausgabeverantwortlichen gemäß Kapitel
1328 1.6 entgegen und erzeugt die beauftragten CV-Zertifikate. Pro Datensatz des
1329 Herausgabeverantwortlichen gemäß Kapitel 1.6 zu einem öffentlichen Schlüssel
1330 (öffentlicher Schlüssel, CHR und CHAT) werden die erforderlichen Angaben zu einem CV-
1331 Zertifikat zusammengestellt. Hierzu gehören die Daten gemäß [gemSpec_PKI#6.7].

1332 Für die Belegung der Zertifikatsfelder bzw. zur Erzeugung des CV-Zertifikats sind durch
1333 die CVC-CA die folgenden Anforderungen zu erfüllen:

1334 TIP1-A_2673 - Berücksichtigung von Eingangsdaten gemäß [gemSpec_PKI]

1335 Für die Erzeugung des Zertifikats MUSS der TSP-CVC sicherstellen, dass die Festlegungen
1336 gemäß der Spezifikation PKI der TI-Plattform [gemSpec_PKI] hinsichtlich der
1337 Zertifikatsprofile, der Object Identifier sowie der Kodierung von Identitäten berücksichtigt
1338 werden.

1339 [\leq]

1340 TIP1-A_2676 - Verwendung der Eingangsdaten

1341 Der TSP-CVC MUSS zur Erzeugung eines CV-Zertifikats die zur Verfügung gestellten
1342 Daten verwenden.

1343 [\leq]

1344 TIP1-A_5378 - Setzen der Certificate Effective Date (CED)

1345 Der TSP-CVC (ausgenommen der TSP-CVC eGK) MUSS bei Erzeugung eines CV-
1346 Zertifikats für die Kartengeneration 2₇ als Certificate Effective Date (CED) ein durch den
1347 Kartenherausgeber oder durch einen von ihm benannten Dritten definiertes Startdatum
1348 eintragen. Für Komponentenzertifikate wird das Startdatum durch den TSP-CVC
1349 festgelegt.

1350 [\leq]

1351 TIP1-A_5379 - Setzen der Certificate Expiration Date (CXD)

1352 Der TSP-CVC MUSS bei Erzeugung eines CV-Zertifikats für die Kartengeneration 2 als
1353 Certificate Expiration Date (CXD) ein Datum einstellen, das die Gültigkeitsdauer des CV-
1354 Zertifikats in Abhängigkeit der Kartenart festlegt und die in Tab_PKI_950 definierten
1355 maximalen Gültigkeitsdauern einhält.

1356 [\leq]

1357 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 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.

5.1.2.2 Card Holder Authorization Template (CHAT)

CV-Zertifikate der Kartengeneration 2 enthalten das Card Holder Authorization Template (CHAT). Die sog. Flagliste (flagList) im Feld CHAT steuert die Zugriffsberechtigung einer Karte auf die Inhalte einer anderen Karte (z.B. HBA auf eGK). Festlegungen zu CHAT werden detailliert in [gemSpec_PKI#6.7] beschrieben.

5.1.2.3 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.

[<=]

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 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.

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.

[<=]

1420

6 Anhang – Verzeichnisse

1421

6.1 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

6.2 Glossar

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

6.3 Abbildungsverzeichnis

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

6.4 Tabellenverzeichnis

~~Tabelle 1: Tab_PKI_950 Maximale Gültigkeitsdauern von CV-Zertifikaten 38~~

Tabelle 1: Tab_PKI_950 Maximale Gültigkeitsdauern von CV-Zertifikaten 38

|

1430 6.5 Referenzierte Dokumente

1431 6.5.1 Dokumente der gematik

1432 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 1433 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
 1434 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
 1435 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und
 1436 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
 1437 aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in
 1438 der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der
 1439 die vorliegende Version aufgeführt wird.
 1440

[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
[gemZul_Prod_CVC]	gematik: Verfahren Beschreibung – Zulassung Produkte der Telematikinfrastruktur: TSP-CVC

1441 6.5.2 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.

1442