SRQ-ID: 1201

Betrifft:

Themenkreis	PKI und Zertifikate
Schlagwort	
zu Dokument / Datei (evtl. ersetzt SRQ)	gemPKI_Reg, ersetzt SRQ 0911
Version	1.5.0
Bezug (Kap., Abschnitt, Tab., Abb.)	3, 4, 5, 6, 7, A

Stichwort: Anpassung an normativen Vorgaben und Änderungen/Ergänzungen für Basis-Rollout

Frage:

Welche Änderungen der Dokumentversion 1.5.0 ergeben sich durch Anpassung an die normativen Vorgaben? Welche zusätzlichen Änderungen/Ergänzungen werden für den Basis-Rollout vorgenommen?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz	Die SRQ ist für alle Zulassungen zu beachten, die nach dem 07.04.2011 beantragt werden.		
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	offen	voraussichtl. Zeitpunkt	
Anmerkungen:	Dieser SRQ enthält unter anderem Maßnahmen, die sich aus dem Sicherheitsgutachten ergeben haben.		
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Es wurden folgenden Änderungen/Ergänzungen vorgenommen:

- Die Tabelle der bereits erfassten Eingangsanforderungen wurde durch die Streichung der Anforderung A_00824 angepasst.
  (Abschnitt 3)
- Die Interoperabilität zwischen Kartengenerationen wurde angepasst.
  (Abschnitt 4.2)
- Die Begrifflichkeit wurde in Bezug auf die Authentisierung festgelegt. „Authentisierung einer Funktionseinheit“ ersetzt „Authentisierung eines Gerätes“.
  (Abschnitt 4.4)
- Eine Aussage zur Verwendung des Zugriffsprofil 0 bei HBA und SMC wurde korrigiert.
  (Abschnitt 4.4)
- Die Festlegung zu Karten mit mehr als einem CV-Zertifikat wurde korrigiert.
  (Abschnitt 4.5.4).
- Es wurden Hinweise auf das Gültigkeitsende bei Chipkarten und Schlüsselpaaren eingefügt. Aussagen über die Zuständigkeiten der Karteninhaber SMC-K und SMCRFID wurden angepasst.
  (Abschnitte 4.5.3, 4.5.7, 4.5.8 und 4.8.5)
- Die Aussage zur Sperrbarkeit von CV-Zertifikaten wurde präzisiert.
  (Abschnitt 4.8.4)
- Dier Anforderungen an Sicherheitsgutachten wurden ergänzt.
  (Abschnitt 5.2.1)
- Es wurden Anforderungen zur Identifizierung des Antragstellers einer PKI-Registrierung (TSP CVC-Sub-CA) aufgenommen.
  (Abschnitte 5.2.1, 5.2.3, 5.2.5, 5.3.1 und 5.3.4)
- Die Ablaufbeschreibung des Registrierungsprozesses wurde korrigiert und ergänzt.
  (Abschnitte 5.2.2, 5.2.3, 5.3.2, 5.3.3 und 5.3.4)
- Die Lebensdauer der Schlüssel wurde in Bezug auf eine Weiterverwendung des Schlüsselpaares gemäß des [gemSiKo] und [gemSpec_Krypt] angepasst.
  (Abschnitt 5.2.5)
- Eine Aussage zur Qualifizierung eines Betreibers wurde präzisiert.
  (Abschnitt 6.3)
- Es wurden Anforderungen zur Absicherung der Authentizität des öffentlichen Schlüssels der CVC-Root-CA aufgenommen.
  (Abschnitt 6.5)
- Die Bezeichner für Informationsobjekte wurden ergänzt.
  (Abschnitt 6.6.1)

- Es wurde eine Einschränkung der Schlüsselnutzung vorgenommen.
  (Abschnitt 6.6.3)
- Die Festlegung des Levels (Prüftiefe) für Zertifizierung nach FIPS 140-2 wurde ergänzt.
  (Abschnitt 6.6.5.)
- Eine Referenz auf gemSiko wurde korrigiert.
  (Abschnitt 6.6.9)
- Es wurden Anforderungen zur Umsetzung des 4-Augen-Prinzips für den Prozess der Ausstellung des Zertifikats der CVC-CA der zweiten Ebene aufgenommen.
  (neuer Abschnitt 6.6.10).
- Es wurden Anforderungen bzgl. der Mitteilung der registrierten Antragssteller an den Betreiber der CV-Root-CA aufgenommen.
  (Abschnitt 7.2.2)
- Hinweise auf die OID für das Cha-Attribut wurden gestrichen.
  (Abschnitt 7.3.1)
- Die zusätzlichen normativen Vorgaben dieser Spezifikation wurden in Bezug auf das Parameter CHA angepasst.
  (Abschnitt A2.2)
- Die Begrifflichkeit („Authentisierung einer Funktionseinheit“ statt „Authentisierung eines Gerätes“) und der Verteilung der Zugriffsprofile auf die verschiedenen Arten von Chipkarten wurden überarbeitet.
  (Abschnitt A3)
- Verteilung der Zugriffsprofile für das Authentisieren einer Funktionseinheit auf die verschiedenen Kartentypen wurde angepasst.
  (Abschnitt A3.2)

3. Anforderungen

…

Tabelle 1: Bereits erfasste Eingangsanforderungen

Quelle	Anforderungsnummer	Anforderungslevel	Beschreibung
[…]			
AM	A_00823	MUSS	Der dezentrale Speicherort privater Schlüssel MUSS nach der initialen Aufbringung der CVC-Zertifikate vor Veränderung geschützt werden
~~AM~~	~~A_00824~~	~~MUSS~~	~~Nicht mehr gültige private CVC-Schlüssel MÜSSEN dauerhaft und nachweislich vom weiteren Gebrauch ausgeschlossen werden (z.B. durch dokumentierte Vernichtung des Trägermediums)~~
AM	A_01108	MUSS	Verwendung von X.509 und CVC Zertifikaten Die PKI MUSS eine Infrastruktur für X.509 und Card-verifiable-Certificates (CV Zertifikate) mit …
[…]			

4.2 Interoperabilität zwischen Kartengenerationen

Aktuell werden für die Chipkarten der Telematikinfrastruktur die drei Generationen G0, G1 und G2 geführt. Bezüglich der C2C-Authentikation zwischen Chipkarten legt die Generation einer Chipkarte dabei die zu verwendenden Algorithmen und die Längen der beteiligten Schlüssel fest. Siehe [gemSpec_Krypt#5.1.2.1] für die normativen Vorgaben für die Generation G1. Folgende Tabelle zeigt die aktuellen Vorgaben im Überblick:

Tabelle 2: Schlüsselanforderungen für die Kartengenerationen der Gesundheitstelematik

Generation	Basis für Signaturalgorithmus	Schlüssellänge	Hashalgorithmus
G0	RSA	1024	SHA-1
G1	RSA	2048	SHA-256
G2	elliptische Kurven	noch nicht entschieden	noch nicht entschieden

Zwischen zwei Chipkarten~~, die zu verschiedenen Generationen gehören,~~ kann keine direkte C2C-Authentikation erfolgreich durchgeführt werden, falls diese dabei Schlüssel unterschiedlicher Länge oder unterschiedliche Algorithmen einsetzen.

Für jede Generation wird eine eigene CVC-PKI aufgebaut. Der Betreiber der Root-CVC-CA wird für jede Generation eine eigene Root-CVC-CA betreiben. Das gleiche gilt für eine CVC-CA der zweiten Ebene, sofern sie CV-Zertifikate für Chipkarten verschiedener Generationen erzeugen will.

[...]

4.4 Zugriffsprofile

Jedes CV-Zertifikat einer Chipkarte (eGK, HBA, SMC) enthält ein Zugriffsprofil. Dabei wird zwischen Zugriffsprofilen für eine

- Authentisierung einer Rolle und Zugriffsprofilen für eine
- Authentisierung einer Funktionseinheit eines Gerätes

unterschieden.

Begrifflichkeit:

- CV-Zertifikate mit einem Zugriffsprofil für eine Rollenauthentisierung werden auch als CV-Rollen-Zertifikat bezeichnet.
- CV-Zertifikate mit einem Zugriffsprofil für eine ~~Geräteauthentisierung~~ Authentisierung einer Funktionseinheit eines Gerätes werden auch als CV-Geräte-Zertifikat bezeichnet.

Bezüglich der Verteilung der verschiedenen CV-Zertifikate auf die Typen von Chipkarten gilt aktuell das Folgende:

- eGKs enthalten nur ein CV-Rollen-Zertifikat.
- SMC-Ks und SMC-RFIDs enthalten nur (ggf. mehrere) CV-Geräte-Zertifikate.
- HBAs, SMC-As und SMC-Bs enthalten sowohl ein CV-Rollen-Zertifikat als auch (ggf. mehrere) CV-Geräte-Zertifikate.

Bei einem HBA, einer SMC-A und einer SMC-B wird vorausgesetzt, dass sowohl das CV-Rollen-Zertifikat als auch die CV-Geräte-Zertifikate von der gleichen CVC-CA erzeugt wurden.

Authentisierung einer Rolle: Für ein CV-Rollen-Zertifikat, das in einer eGK, einem HBA oder einer SMC-A/SMC-B enthalten ist, gibt das Zugriffsprofil an, welche Rolle der Karteninhaber (Person bzw. Organisation) hat. Über die in dem CV-Zertifikat enthaltene Rolle wird festgelegt, welche Zugriffsrechte der Karteninhaber nach einer C2C-Authentikation auf die in der anderen Chipkarte gespeicherten Daten erhält.

Authentisierung einer Funktionseinheit eines Gerätes: Für ein CV-Geräte-Zertifikat, das in einem HBA, einer SMC-A, einer SMC-B, einer SMC-K oder SMC-RFID enthalten

ist, gibt das Zugriffsprofil an, ~~zu welchem Gerätetyp die Chipkarte gehört~~ dass die Chipkarte die entsprechende Funktionseinheit enthält.

Aktuell werden für die Rollenauthentisierung die Zugriffsprofile 0 bis 9 unterschieden. ~~Die die Geräteauthentisierung~~ Für die Authentisierung von Funktionseinheiten werden aktuell die Rollen 51 bis 55 unterschieden. Siehe auch Anhang A.3.

Eine eGK erhält immer ein CV-Rollen-Zertifikat mit dem Zugriffsprofil 0. Der Inhaber einer eGK erhält damit durch eine C2C-Authentikation keine weiteren Zugriffsrechte auf Daten, die in der anderen Chipkarte (HBA/SMC-A/SMC-B) gespeichert sind.

Ein HBA bzw. eine SMC-A/SMC-B erhält immer ein CV-Rollen-Zertifikat mit einem Zugriffsprofil, das der Rolle des Karteninhabers (Person bzw. Organisation der Leistungserbringer) entspricht. Bei einem HBA und einer SMC ~~SMC-A~~ hat das Zugriffsprofil dabei immer einen Wert ungleich 0~~, bei einer SMC-B kann dagegen das Zugriffsprofil auch den Wert 0 enthalten~~. Der Inhaber des HBA bzw. der SMC-A/SMC-B erhält damit durch eine C2C-Authentikation (abhängig von dem konkreten Zugriffsprofil) Zugriffsrechte auf weitere Daten, die in der anderen Chipkarte (eGK) gespeichert sind. Das konkrete Zugriffsprofil für ein CV-Zertifikat in einer HBA bzw. einer SMC ist dabei abhängig von der Berufsgruppe, zu der der Karteninhaber gehört. Die Zuordnung der Profile zu den einzelnen Berufsgruppen bzw. Organisationen der Leistungserbringer ist nicht Gegenstand dieses Dokuments.

CV-Zertifikate, die durch die Root-CVC-CA für eine CVC-CA ausgestellt werden, enthalten kein Zugriffsprofil.

[...]

4.5.3 Kartenherausgeber

Der Herausgeber von eGK/HBA/SMC beauftragt eine CVC-CA, die für seine Chipkarten benötigten CV-Zertifikate zu generieren. Er beauftragt nur solche CVC-CAs, für die aktuell eine gültige Registrierung durch die gematik vorliegt.

Der Herausgeber ist dabei dafür verantwortlich, dass

- ein CV-Rollen-Zertifikat für eine Chipkarte das korrekte Zugriffsprofil (d.h. für eine eGK das Zugriffsprofil 0 und für eine HBA/SMC ein Zugriffsprofil ungleich 0) hat, das zu der Rolle des Karteninhabers gehört,
- ein CV-Geräte-Zertifikat für eine Chipkarte das korrekte Zugriffsprofil hat, das zu dem Gerätetyp der Chipkarte gehört,
- in dem CV-Zertifikat für eine eGK, einen HBA bzw. eine SMC die korrekte ICCSN der Chipkarte in das Feld CHR eingetragen wird,
- der zu dem durch das CV-Zertifikat zertifizierte öffentliche Schlüssel gehörende private Schlüssel, in der eGK,HBA oder SMC gespeichert ist und nur dort.

Nach Ablauf der Gültigkeitsdauer einer Chipkarte bzw. nach Ablauf der Gültigkeit eines Schlüsselpaares MUSS die Einsetzbarkeit der Chipkarte 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 Kartenherausgeber vorgegeben. Der Kartenherausgeber MUSS den Karteninhaber zu einem geeigneten Mitwirken hierbei verpflichten. Ein Einzug einer Chipkarte durch den Kartenherausgeber MUSS durch diesen protokolliert werden.

Für die Ausgabe von HBAs und SMCs können weitere Anforderungen durch die jeweils zuständige berufsständische Organisation vorgegeben werden.

Der Kartenherausgeber kann seine Verantwortlichkeiten nur in Zusammenarbeit mit dem Kartenhersteller und der CVC-CA erfüllen. Siehe dazu Abschnitt 6.5.

4.5.4 CVC-CA

[...]

Für die Erzeugung von CV-Geräte-Zertifikate mit einem Zugriffsprofil ungleich 0 benötigt die CVC-CA keine besondere Qualifizierung.

Für den Fall, dass eine eGK, ein HBA oder eine SMC zwei oder mehr CV-Zertifikate für Authentisierungszwecke enthält, MUSS der Kartenherausgeber sicherstellen, dass diese CV-Zertifikate von derselben CVC-CA herausgegeben werden. Diese Tatsache muss nicht von der Karte überprüfbar sein bzw. überprüft werden.

[…]

4.5.7 Karteninhaber (HBA, SMC-A, SMC-B)

[...]

Für eine SMC-A bzw. SMC-B gilt im Rahmen der PKI für CV-Zertifikate das gleiche wie für einen HBA.

Nach Ablauf der Gültigkeitsdauer einer Chipkarte bzw. nach Ablauf der Gültigkeit eines Schlüsselpaares muss die Einsetzbarkeit der Chipkarte 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 Kartenherausgeber vorgegeben. Siehe dazu Abschnitt 4.5.3. Der Karteninhaber ist verpflichtet, hierbei gemäß den Vorgaben des Kartenherausgebers mitzuwirken.

4.5.8 Karteninhaber (SMC-K, SMC-RFID)

Eine SMC-K ~~bzw. eine SMC-RFID~~ enthält nur ein CV-Geräte-Zertifikat, die SMC-RFID kann auch zwei CV-Geräte-Zertifikate enthalten. Durch eine C2C-Authentikation mit einer anderen Chipkarte erhalten die SMC-K/SMC-RFID und damit ihr Karteninhaber keine weiteren Zugriffsrechte auf in der anderen Chipkarte gespeicherten Daten.

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

Im Rahmen der PKI für CV-Zertifikate hat ein Inhaber einer SMC-K die Verpflichtung, den Verlust seiner SMC-K unverzüglich zu melden. Konkrete Festlegungen hierzu werden durch die ausgebende Organisation geregelt.

Der Inhaber einer SMC-RFID hat die Verpflichtung beim Verlust seiner SMC-RFID, das Pairing zum Auslösen der Komfortsignatur zurückzusetzen, siehe auch [gemSpec_Kon#4.1.3.4.3.3].

Nach Ablauf der Gültigkeitsdauer einer Chipkarte bzw. nach Ablauf der Gültigkeit eines Schlüsselpaares muss die Einsetzbarkeit der Chipkarte 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 Kartenherausgeber vorgegeben. Siehe dazu Abschnitt 4.5.3. Der Karteninhaber ist verpflichtet, hierbei gemäß den Vorgaben des Kartenherausgebers mitzuwirken.

4.8.4 Sperrung eines CV-Zertifikats

CV-Zertifikate können (gemäß der Gesamtarchitektur [gemGesArch#8.4.4]) nicht gesperrt werden. Muss die Einsetzbarkeit eines CV-Zertifikats bei Vorliegen eines schwerwiegenden Problems beendet werden, kann dies nur durch Einziehen und Zerstören der zugehörigen Chipkarte erreicht werden.

4.8.5 Lebensdauer eines CV-Zertifikats

CV-Zertifikate haben nach ihrer Generierung theoretisch eine unbegrenzte Lebensdauer. Die Einsetzbarkeit eines CV-Zertifikats wird aber durch die Lebensdauer des zugehörigen privaten Schlüssels begrenzt. Gemäß [gemSpecKrypt#5.1.2.1] soll die Lebensdauer des zugehörigen privaten Schlüssels 5 Jahre nicht überschreiten. Die Einschränkung der Lebensdauer des privaten Schlüssels wird wiederum durch die Gültigkeitsdauer der Chipkarte realisiert.

Nach Ablauf der Gültigkeitsdauer einer Chipkarte bzw. nach Ablauf der Gültigkeit eines Schlüsselpaares MUSS die Einsetzbarkeit der Chipkarte dauerhaft und nachweislich bezüglich der durch die CV-Zertifikate geschützten Anwendungen unterbunden werden. Dies KANN z. B. durch Einzug der Chipkarte durch den Kartenherausgeber realisiert werden. Ein entsprechender Einzug einer Chipkarte MUSS protokolliert werden.

5.2 Verfahren für eine Produktiv-CVC-CA

5.2.1 Antrag auf Registrierung

[...]

Die Kopie des Registerauszugs muss von dem aktuellen Eintrag des Betreibers in dem zuständigen Register (Handelsregister, Vereinsregister, etc.) stammen. Aus diesem müssen die folgenden Informationen hervorgehen:

- Hauptsitz des Betreibers (Einschränkungen siehe 5.1.1),
- Gesellschafter des Betreibers,
- Zeichnungsberechtigte Personen.

Das Sicherheitsgutachten muss bestätigen, dass der Betreiber der CVC-CA die Mindestanforderungen aus Abschnitt 6.6 erfüllt und dies in einem Sicherheitskonzept (gemäß den Anforderungen aus dem Abschnitt 6.1 und [gemSiKo#8.6]) ausreichend beschrieben hat. Das Sicherheitsgutachten muss von einem durch die gematik anerkannten Gutachter stammen. Bei akkreditierten CAs bestätigt die Selbsterklärung, dass der Betrieb CVC unter denselben Sicherheitsbedingungen erfolgt.

Die Anzahl der notwendigen Qualifizierungsnachweise hängt von den Profilen ab, mit denen die CVC-CA CV-Zertifikate erzeugen wird. Ein Qualifizierungsnachweis muss dabei von der für das Profil zuständigen berufsständischen Organisation stammen.

Alle Formulare des Antrages und die beigefügten Unterlagen MÜSSEN ~~müssen~~ rechtsverbindlich und konsistent zu den Angaben im Handelsregisterauszug ~~nach Registerauszug~~ unterschrieben sein. Es muss überprüft werden, ob die unterzeichnende Person gemäß Handelsregisterauszug eine Zeichnungsbefugnis für das entsprechende Unternehmen besitzt. Falls Nein, darf der Antrag nicht weiter bearbeitet werden und das ISMS der gematik muss über den Vorfall informiert werden.

Um sicher zu stellen, dass es sich beim unterzeichnenden Antragssteller auch wirklich um die behauptete Person handelt, MUSS diese sicher identifiziert werden. Zudem muss sichergestellt werden, dass die Integrität und Authentizität des Antrags nicht verletzt wurde, also auch genau der Antrag bearbeitet wird, den der Antragsteller intendiert hat.

Die Registrierungsstelle der gematik MUSS für die sichere Identifizierung des zeichnungsberechtigten Antragsstellers mindestens eines der folgenden, grundsätzlich geeigneten, Verfahren einsetzen:

(1) Persönliche Übergabe
Hierbei erfolgt die persönliche Übergabe des Antrags durch den Antragsteller an die zuständigen Mitarbeiter in der gematik und die Identifikation per Personalausweis oder Reisepass durch die Mitarbeiter der gematik. Der zuständige Mitarbeiter der gematik muss die Unterschrift des Antrags mit der Unterschriftenprobe auf dem präsentierten Ausweisdokument vergleichen. Die festgestellte Identität wird anschließend mit den Angaben im Handelsregisterauszug verglichen und damit überprüft, ob die identifizierte Person zeichnungsbefugt ist.

(2) Nutzung des Postident-Verfahrens
Hierbei übersendet der Antragsteller den Antrag und die notwendigen Unterlagen im Rahmen des Postident-Verfahrens an die Registrierungsstelle der gematik. Er muss sicherstellen, dass die Integrität der übergebenen Dokumente bis zum Zeitpunkt der Übergabe an die das Postident-Verfahren durchführende Stelle sicher gestellt ist. Bei der Übergabe werden von der das Postident-Verfahren durchführenden Stelle die Identität des Antragstellers per Personalausweis oder Reisepass festgestellt und die abgegebenen, in einem Umschlag verschlossenen,

Unterlagen mit dieser Identität (inkl. einer Unterschriftenprobe) verbunden. Die Unterschrift auf den Antragsunterlagen muss nach Eingang in der Registrierungsstelle von den Mitarbeitern der gematik mit der Unterschriftenprobe aus dem Postident-Verfahren überprüft werden. Die Angaben zur Identität des Antragsstellers aus dem Postident-Verfahren werden mit den Angaben im Handelsregisterauszug verglichen und überprüft, ob die entsprechende Person zeichnungsbefugt ist.

(3) Nutzung qualifizierter elektronischer Signaturen
Hier wird der Antrag per qualifizierter elektronischer Signatur vom Antragsteller unterschieben. Die Signatur des Antrags muss von den Mitarbeitern der gematik überprüft werden. So wird die Integrität und die Authentizität (bez. der den Antrag stellenden Person) des Antrags sichergestellt. Die Mitarbeiter der gematik müssen anhand der im qualifizierten Zertifikat enthaltenden Angaben überprüfen, ob es sich bei der mit dem Zertifikat verbundenen natürlichen Person um dieselbe Person handelt, die im Handelsregisterauszug als zeichnungsberechtigte Person aufgeführt ist.

Weitere Hinweise zur Verwendung erhalten Sie auf der Homepage der gematik (www.gematik.de) unter der Rubrik „Zertifikatsherausgeber“.

5.2.2 Entscheidung über die Registrierung

Über eingehende Anträge auf Registrierung einer Produktiv-CVC-CA entscheidet die gematik nach Eingang des schriftlichen Antrags innerhalb von fünfzehn Werktagen. Zur Fristwahrung gilt das Datum des Poststempels bei der Einsendung der Unterlagen im Papierformat.

Ein Antrag auf Registrierung einer Produktiv-CVC-CA wird positiv entschieden, falls

- der Antrag gemäß den Vorgaben in Abschnitt 5.2.1 vollständig ist,
- die Kontrolle des Registerauszuges bei dem zuständigen Register die Korrektheit und Aktualität der Kopie bestätigt,
- [...]

[...]

5.2.3 Änderung einer Registrierung

Der Betreiber einer registrierten Produktiv-CVC-CA ist verpflichtet, Änderungen an den für die Registrierung relevanten Informationen unverzüglich der gematik mitzuteilen (Formular "Änderungsmitteilung").

Zurzeit sind die folgenden Änderungen mitteilungspflichtig:

- Einstellung des Betriebs,
- Änderungen an der Gesellschafterstruktur,
- Änderungen bei den zeichnungsberechtigten Personen,

- Verlagerung des Hauptsitzes des Betreibers bzw. der eigentlichen Betriebsstätte der Produktiv-CVC-CA in ein anderes Land,
- Änderungen bei der Zuordnung von Mitarbeitern zu den Rollen "Leiter CA", "Sicherheitsbeauftragter" oder "Antragsteller CA-CV-Zertifikat",
- [...]

[...]

Sollen zukünftig CV-Zertifikate mit neuen Profilen erzeugt werden, müssen die entsprechenden Qualifizierungsnachweise der Änderungsmitteilung beigefügt werden.

Ggf. können die Änderungen zu einem Widerruf der Registrierung führen (siehe Abschnitt 5.2.4).

~~Alle Formulare des Antrages und die beigefügten Unterlagen müssen rechtsverbindlich nach Registerauszug unterschrieben sein.~~

Alle Formulare des Antrages auf Änderung einer Registrierung und die beigefügten Unterlagen MÜSSEN rechtsverbindlich und konsistent zu den Angaben im Handelsregisterauszug von einer zeichnungsberechtigten Person unterschrieben sein.

Für die Identifizierung des Antragstellers gelten dieselben Vorgaben wie bei der erstmaligen Registrierung (siehe Abschnitt 5.2.1).

[…]

5.2.5 Verlängerungsantrag

Die Gültigkeitsdauer der Registrierung einer Produktiv-CVC-CA beträgt 2 Jahre. Spätestens 3 Monate vor Ablauf muss die registrierte CVC-CA einen Verlängerungsantrag stellen. Dieser bestätigt, dass der Betrieb weiterhin unter den bei der erstmaligen Registrierung nachgewiesenen Sicherheitsbedingungen durchführt wird. Das Formular muss vollständig ausgefüllt werden. Unter diesen Voraussetzungen kann das Schlüsselpaar weiter verwendet werden, wobei jedoch die maximale Lebensdauer der Schlüssel gemäß [gemSpec_Krypt#5.1.2.2] (basierend auf [gemSiKo#AnhF]) 5 Jahre nicht überschreiten darf.

Alle Formulare des Antrages auf Verlängerung einer Registrierung und die beigefügten Unterlagen MÜSSEN rechtsverbindlich unterschrieben sein.

Der Antrag auf Verlängerung der Registrierung einer Produktiv-CVC-CA KANN (abweichend zum Vorgehen der erstmaligen Registrierung) von dem benannten „Leiter CVC CA“ gestellt werden. Für die Identifizierung des Antragstellers gelten dieselben Vorgaben wie bei der erstmaligen Registrierung (siehe Abschnitt 5.2.1).

5.3 Verfahren für eine Test-CVC-CA

5.3.1 Antrag auf Registrierung

[...]

Die Kopie des Registerauszugs muss von dem aktuellen Eintrag des Betreibers in dem zuständigen Register (Handelsregister, Vereinsregister, etc.) stammen. Aus diesem müssen die folgenden Informationen hervorgehen:

- Hauptsitz des Betreibers (Einschränkungen siehe 5.1.1),
- Gesellschafter des Betreibers,
- zeichnungsberechtigte Personen

Alle Formulare des Antrages und die beigefügten Unterlagen MÜSSEN ~~müssen~~ rechtsverbindlich und konsistent zu den Angaben im Handelsregisterauszug ~~nach Registerauszug~~ unterschrieben sein.

Für die Identifizierung des Antragstellers gelten dieselben Vorgaben wie bei Registrierung einer Produktiv-CVC-CA (siehe Abschnitt 5.2.1).

5.3.2 Entscheidung über die Registrierung

Über eingehende Anträge auf Registrierung einer Test-CVC-CA entscheidet die gematik nach Eingang des Antrages innerhalb von fünfzehn ~~fünf~~ Werktagen. Zur Fristwahrung gilt das Datum des Poststempels bei der Einsendung der Unterlagen im Papierformat.

Ein Antrag auf Registrierung eines Betreibers einer Test-CVC-CA wird positiv entschieden, falls

- der Antrag gemäß den Vorgaben in Abschnitt 5.3.1 vollständig ist
- die Kontrolle des Registerauszuges bei dem zuständigen Register die Korrektheit und Aktualität der Kopie bestätigt und
- keine sonstigen Gründe gegen die Registrierung bestehen.

5.3.3 Widerruf der Registrierung

[...]

Der Widerruf der Registrierung der Test-CVC-CA kann durch die gematik ohne erneute Rücksprache mit dem Betreiber erfolgen. Der Betreiber wird über den Widerruf informiert.

Die gematik behält sich den Widerruf von Test-CVC-CA-Registrierungen ausdrücklich vor.

5.3.4 Änderung der Registrierung

Der Betreiber einer zugelassenen Test-CVC-CA ist verpflichtet, Änderungen an den für die Registrierung relevanten Informationen unverzüglich der gematik mitzuteilen (Formular "Änderungsmitteilung Registrierung").

Zurzeit sind die folgenden Änderungen mitteilungspflichtig:

- Einstellung des Betriebs,
- Änderungen an der Gesellschafterstruktur,
- Änderungen bei den zeichnungsberechtigten Personen,
- Verlagerung des Hauptsitzes des Betreibers bzw. der eigentlichen Betriebsstätte der Test-CVC-CA in ein anderes Land,
- Änderungen bei der Zuordnung von Mitarbeitern zu den Rollen "Leiter CA", "Sicherheitsbeauftragter" oder "Antragsteller CA-CV-Zertifikat",

Das Formular ist als PDF-Formular konzipiert. Es kann von der gematik-Website herunter geladen werden und ist elektronisch auszufüllen. Es MUSS (direkt aus dem Formular heraus) per Mail vorab an die gematik gesendet werden. Der mit dem Mailversand erstellte Ausdruck ist dann unterschrieben (s. u.) per Post zu senden. Die Änderungen sind durch entsprechende Nachweise, z. B. neuer Registerauszug, vorzulegen. Gegebenfalls können die Änderungen zu einem Widerruf der Betreiber-Registrierung führen (siehe Kapitel 5.2.1.4).

Alle Formulare des Antrages auf Änderung einer Registrierung und die beigefügten Unterlagen MÜSSEN rechtsverbindlich und konsistent zu den Angaben im Handelsregisterauszug von einer zeichnungsberechtigten Person unterschrieben sein.

Für die Identifizierung des Antragstellers gelten dieselben Vorgaben wie bei der erstmaligen Registrierung (siehe Abschnitt 5.2.1).

6.3 Anforderungen an eine HBA-/SMC-Qualifizierung

[...]

Eine CVC-CA darf CV-Zertifikate für einen HBA bzw. eine SMC nur mit solchen Zugriffsprofilen (letztes Byte in dem Feld CHA) erzeugen, für die bei der Registrierung (5.2.1) bzw. bei einer späteren Änderung der Registrierung (5.2.3) die notwendigen Berechtigungsnachweise ~~Qualifizierungsnachweise~~ der zuständigen berufsständischen Organisationen vorgelegen haben. Abweichungen hiervon führen zu einem unverzüglichen Widerruf der Registrierung.

Alle Anforderungen an eine Produktiv-CVC-CA für eine Qualifizierung sowie das Vorgehen für ihre Durchführung werden durch die zuständige berufsständische Organisation geregelt.

Für die Registrierung einer Test-CVC-CA ist eine Qualifizierung noch nicht notwendig. Diese muss erst nachgewiesen werden bei der Registrierung einer Produktiv-CVC-CA.

6.5 Zusammenspiel Kartenherausgeber, CVC-CA, Kartenhersteller

Bei dem Prozess für die Herstellung einer Chipkarte (eGK, HBA, SMC) 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 Aufgabenteilung denkbar.

Für die Sicherheit der PKI für CV-Zertifikate müssen die folgenden Ziele erreicht werden:

- [...]
- Ein privater Schlüssel DARF NIE in zwei verschiedenen Chipkarten verwendet werden.
- In die Chipkarte muss der korrekte aktuelle öffentliche Schlüssel der (Produktiv-/ Test-) Root-CVC-CA eingebracht werden ([gemSiKo#B4.5.3]).

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

  Jeder Akteur, der den öffentlichen Schlüssel der CVC-Root-CA verwendet, MUSS die Authentizität dieses Schlüssel vor dessen Verwendung, zum Beispiel beim Einbringen dieses Schlüssels in das Personalisierungssystem bzw. beim Zugriff auf diesen Schlüssel im Personalisierungssystem, sicherstellen. Dabei MUSS der Akteur durchgängig das 4-Augen-Prinzip umsetzen. Die Umsetzung MUSS in einem entsprechenden Organisationskonzept als Teil des Sicherheitskonzepts beschrieben sein.
- In die Chipkarte muss das korrekte CA-CV-Zertifikat der CVC-CA eingebracht werden, die das enthaltene CV-Zertifikat erzeugt hat ([gemSiKo#B4.5.3]).
- [...]

[...]

6.6 Mindestanforderungen an eine CVC-CA

6.6.1 Schutzbedarfsfeststellung

Der Schutzbedarf für die für eine Produktiv-CVC-CA relevanten kryptographischen Objekte wird durch [gemSiKo] in den folgenden Abschnitten vorgegeben:

Tabelle 2a: Referenzierte Schutzbedarfsfeststellung mit Informationsobjekten (Io)

Objekt	[Referenz]	Io-Nummer
Privater Schlüssel Root-CVC-CA	[gemSiKo#C2.87]	Io122
Öffentlicher Schlüssel/CA-CV-Zertifikat Root-CVC-CA	[gemSiKo#C2.88]	Io123
Privater Schlüssel CVC-CA	[gemSiKo#C2.89]	Io124
Öffentlicher Schlüssel/CA-CV-Zertifikat CVC-CA	[gemSiKo#C2.90]	Io125
Privater Schlüssel eGK für C2C-Auth.	[gemSiKo#C2.59]	Io083

Objekt	[Referenz]	lo-Nummer
Öffentlicher Schlüssel/CV-Zertifikat eGK	[gemSiKo#C2.24]	lo097
Privater Schlüssel HBA für C2C-Auth.	[gemSiKo#C2.60]	lo084
Öffentlicher Schlüssel/CV-Zertifikat HBA	[gemSiKo#C2.27]	lo096
Privater Schlüssel SMC-A für C2C-Auth.	[gemSiKo#C2.65]	lo091
Öffentlicher Schlüssel/CV-Zertifikat SMC-A	[gemSiKo#C2.64]	lo090
Privater Schlüssel SMC-B für C2C-Auth.	[gemSiKo#C2.69]	lo095
Öffentlicher Schlüssel/CV-Zertifikat SMC-B	[gemSiKo#C2.68]	lo094
Privater Schlüssel SMC-K für C2C-Auth.	[gemSiKo#7.3] Datenklasse DK 11b	
Öffentlicher Schlüssel/CV-Zertifikat SMC-K	[gemSiKo#7.3] Datenklasse DK 9	
Privater Schlüssel SMC-RFID für C2C-Auth.	[gemSiKo#7.3] Datenklasse DK 11b	
Öffentlicher Schlüssel/CV-Zertifikat SMC-RFID	[gemSiKo#7.3] Datenklasse DK 9	

Besondere Schutzbedarfsanforderungen für eine Test-CVC-CA werden nicht vorgegeben.

[…]

6.6.3 Ausschließlichkeit der Schlüsselnutzung

Das Schlüsselpaar einer CVC-CA, für das durch die Root-CVC-CA ein CA-CV-Zertifikat erstellt wurde, darf durch die CVC-CA ausschließlich für das Erstellen von Signaturen ~~im Rahmen der Generierung~~ von CV-Zertifikaten der für diese CA genehmigten Profile eingesetzt werden.

[…]

6.6.5 Sicherheit des Schlüsselpaares

[...]

Als HSM muss ein Modul (bzw. eine Chipkarte) eingesetzt werden, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde ([gemSiKo#4.1.6(AS_EP_06)]). Als Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder FIPS in Frage.

Die Prüftiefe MUSS mindestens

- FIPS 140-2 Level 3,
- Common Criteria EAL 4 oder

- ITSEC E3 der Stärke „hoch“

entsprechen.

~~Bei der notwendigen Prüftiefe muss berücksichtigt werden, ob und wie weit unberechtigte physische Zugriffe auf das HSM während seiner gesamten Lebensdauer durch weitere organisatorische und bauliche Maßnahmen verhindert werden. Werden entsprechende Zugriffe nicht durch weitere Maßnahmen ausgeschlossen, muss die Prüftiefe mindestens CC EAL 4 (bzw. bei den anderen Evaluierungsschemata vergleichbar) umfassen. Mechanismenstärke (bzw. das Angriffspotential) müssen "hoch" sein.~~

Das Schlüsselpaar verliert seine Gültigkeit, falls

- für seine Aufgaben ein neues Schlüsselpaar generiert und in der CA aktiviert wurde oder
- die Registrierung der CVC-CA durch die gematik widerrufen wurde.

[...]

6.6.9 Betriebliche Anforderungen

[...]

Alle zu der CVC-CA gehörenden Systeme müssen in Betriebsstätten betrieben werden, die konkret in einem Land der Europäischen Union liegen ([gemSiKo#B4.5.3]).

Neben den genannten konkreten Vorgaben MÜSSEN auch die übergeordneten Vorgaben aus [gemSiKo#AnhG] bei dem Betrieb einer CVC-CA berücksichtigt werden.

6.6.10 Authentizität des öffentlichen Schlüssels der CVC-CA

Der Betreiber der CVC-Root-CA MUSS 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 4-Augen-Prinzip umsetzen.

Ziel ist es sicher zu stellen, dass innerhalb des Prozesses für die Zertifikatsausstellung notwendige Informationen durch einen Angreifer nicht ausgetauscht werden können (bspw. der mit dem Zertifikat zu verbindende öffentliche Schlüssel). Ansonsten könnten gültige (nicht mehr widerrufbare/sperrbare) CV-Zertifikate für einen Angreifer erzeugt werden.

Der Betreiber einer CVC-Sub-CA MUSS für den Gesamtprozess der Beantragung und des Erhalts eines CVC-Sub-CA-Zertifikats bei einer Root-CVC-CA das 4-Augen-Prinzip umsetzen.

Dies kann bspw. dadurch erfolgen, dass den Zertifikatsausstellungsantrag zwei Mitarbeiter der Sub-CA auf Korrektheit direkt vor der Abgabe an den Betreiber der Root-CA im 4-Augen-Prinzip prüfen und diese Prüfung dokumentieren.

Bei erfolgreicher Ausstellung des beantragten Zertifikats MÜSSEN wieder min. zwei Mitarbeiter der Sub-CA das von der Root-CA übergebene Zertifikat auf Konsistenz bez. des Zertifikatsausstellungsantrags prüfen und dies inkl. Prüfergebnis dokumentieren.

Für fehlgeschlagene Prüfergebnisse MÜSSEN Notfallmaßnahmen im Sicherheitskonzept des Betreibers der Sub-CA definiert und im Eintrittsfalle eingeleitet werden.

Das bei Ausstellung eines Zertifikats durch die CVC-Root-CA angewandte 4-Augen-Prinzip MUSS mit dem 4-Augen-Prinzip der Beantragung und des Erhalts des Zertifikats durch die CVC-Sub-CA so ineinandergreifen, dass die Durchgängigkeit des 4-Augen-Prinzip garantiert ist.

7.2.2 Vorgehen Root-CVC-CA

Nach Eingang eines schriftlichen Antrags führt der Betreiber der Root-CVC-CA die folgenden Überprüfungen durch:

- Liegt für die CVC-CA eine aktuell gültige Registrierung als Produktiv- bzw. Test-CVC-CA vor?
- Stimmen die Angaben zu "Name und Anschrift der CVC-CA" sowie "CA-Name im Zertifikat" mit den Registrierungsdaten überein?
- Ist die genannte Kontaktperson in den Registrierungsdaten enthalten?
- Stammen die Unterschriften von berechtigten Mitarbeitern, die hierfür in den Registrierungsdaten genannt sind?

~~Grundlage für die Überprüfungen ist die aktuelle Liste mit den registrierten CVC-CAs, die die gematik dem Betreiber der Root-CVC-CA regelmäßig zur Verfügung stellt.~~

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

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

7.2.2.1 Übertragung der Liste mit den registrierten CVC-CAs

Grundlage für die Überprüfungen ist die aktuelle Liste mit den registrierten CVC-CAs (siehe [gemSiKo#AnhC2], " Io255 – Liste der registrierten Betreiber einer CA der zweiten Ebene"), die die gematik dem Betreiber der Root-CVC-CA regelmäßig zur Verfügung stellt.

Um sicherzustellen, dass die vom Betreiber der Root-CVC-CA verwendete Liste der bei der gematik vorliegenden aktuellen Liste der registrierten CVC-CAs entspricht, wird diese Liste mindestens bei jeder Änderung und auf Anforderung des Betreibers von der gematik an den Betreiber der Root-CVC-CA übertragen. Dazu MUSS eines der folgenden, geeigneten Verfahren eingesetzt werden. Dieses wird vorab in bilateraler Abstimmung der gematik mit dem Betreiber der Root-CVC-CA festgelegt.

(1) Persönliche Übergabe
Hierbei erfolgt die persönliche Übergabe der Liste der registrierten CVC-CAs durch einen vorher festgelegten Mitarbeiter der gematik an die zuständigen Mitarbeiter des Betreibers der Root-CVC-CA und die Identifikation per Personalausweis oder Reisepass durch den

Betreiber. Der Betreiber der Root-CVC-CA muss die Unterschrift auf jeder Seite der Liste der CVC-CAs mit der Unterschriftenprobe auf dem präsentierten Ausweisdokument vergleichen. Die festgestellte Identität wird anschließend mit den vorab von der gematik hinterlegten Identitäten verglichen und damit überprüft, ob die identifizierte Person zur Aktualisierung der Liste der CVC-CAs berechtigt ist. Der Mitarbeiter der gematik lässt sich den Erhalt der aktuellen Liste der registrierten CVC-CAs ebenfalls vom zuständigen Mitarbeiter des Betreibers der Root-CVC-CA quittieren.

(2) Nutzung qualifizierter elektronischer Signaturen
Hier wird die Liste der registrierten CVC-CAs per qualifizierter elektronischer Signatur von einem vorher festgelegten Mitarbeiter der gematik unterschrieben und dem zuständigen Mitarbeiter des Betreibers der Root-CVC-CA zur Verfügung gestellt. Die Signatur der Liste muss vom Betreiber der Root-CVC-CA überprüft werden. So werden die Integrität und die Authentizität der Liste sichergestellt. Der Betreiber der Root-CVC-CA muss anhand der im qualifizierten Zertifikat enthaltenden Angaben überprüfen, ob es sich bei der mit dem Zertifikat verbundenen natürlichen Person um eine der Personen handelt, die vorab von der gematik als zur Aktualisierung der Liste berechtigt benannt wurden. Der Erhalt der aktuellen Liste der registrierten CVC-CAs wird vom zuständigen Mitarbeiter des Betreibers der Root-CVC-CA durch eine mit qualifizierter Signatur unterschriebene Mitteilung an den vorher festgelegten Mitarbeiter der gematik bestätigt.

7.3.1 CVC-PKCS#10-Request

[...]

Die OIDs für die Attribute sind wie folgt festgelegt:

```
id-cvc-attributes OBJECT IDENTIFIER ::= {
  iso(1) identified-organization(3) dod(6) internet(1)
  private(4) enterprise(1) D-Trust GmbH(4788) 4
}

id-cvc-certificateProfileIdentifier OBJECT IDENTIFIER ::= {
  id-cvc-attributes 1
}

id-cvc-certificateHolderReference OBJECT IDENTIFIER ::= {
  id-cvc-attributes 2
}

id-cvc-CHR-cAName OBJECT IDENTIFIER ::= {
  id-cvc-certificateHolderReference 1
}
id-cvc-CHR-serviceIndicator OBJECT IDENTIFIER ::=  {
  id-cvc-certificateHolderReference 2
}
id-cvc-CHR-keyDicretionaryData OBJECT IDENTIFIER ::= {
  id-cvc-certificateHolderReference 3
}
id-cvc-CHR-algorithmReference OBJECT IDENTIFIER ::= {
  id-cvc-certificateHolderReference 4
}
id-cvc-CHR-yearofActivation OBJECT IDENTIFIER ::= {
  id-cvc-certificateHolderReference 5
}

id-cvc-CertificateHolderAuthorization OBJECT IDENTIFIER ::= {
```

```
  id-cvc-attributes 3
}

id-cvc-CHA-prefix OBJECT IDENTIFIER ::= {
  id-cvc-certificateHolderAuthorization 1
}
id-cvc-CHA-roleID OBJECT IDENTIFIER ::= {
  id-cvc-certificateHolderAuthorization 2
}

id-cvc-algorithmIdentifier OBJECT IDENTIFIER ::= {
  id-cvc-attributes 4
}
```

[...]

A.2.2 – Zusätzliche Vorgaben dieser Spezifikation (normativ)

[...]

CHR

Bei dem Aufbau und der Belegung des Feldes CHR wird unterschieden zwischen einem CV-Zertifikat für eine CVC-CA und einem CV-Zertifikat für eine Chipkarte:

Tabelle 11: Aufbau CHR

CV-Zertifikat für	Länge CHR	Inhalt
CVC-CA	8 Bytes	CAR zu dem Schlüsselpaar
Chipkarte	12 Bytes	'xx xx' || ICCSN der Chipkarte

Für das Feld CHR bei einem CV-Zertifikat für eine Chipkarte gilt das folgende:

- Die ICCSN ist 10 Byte lang und identifiziert eine Chipkarte eindeutig.
- Eine Chipkarte kann auch mehrere Schlüsselpaare für eine C2C-Authentikation (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 Spezifikationen der konkreten Chipkarten festgelegt.

CHA

~~Das Feld CHA existiert nur in einem CV-Zertifikat für eine Chipkarte.~~ Das Feld CHA existiert nur in CV-Rollen-Zertifikaten und CV-Geräte-Zertifikaten. Es ist wie folgt weiter unterteilt:

Tabelle 12: Aufbau CHA

AID	Zugriffsprofil

Es gelten folgende Festlegungen:

- 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. Das Zugriffsprofil MUSS gemäß Anhang A.3.1 bzw. A.3.2 eingetragen werden.

A.3 – Zugriffsprofile

In einem CV-Zertifikat einer Chipkarte ist das Zugriffsprofil dieser Chipkarte enthalten. Dabei wird unterschieden zwischen einem Zugriffsprofil für eine

- Authentisierung einer Rollen (CV-Rollen-Zertifikate) bzw. für eine
- Authentisierung einer Funktionseinheit eines Gerätes (CV-Geräte-Zertifikate).

Bei einem Zugriffsprofil für eine Rollenauthentisierung erhält der Karteninhaber nach einer C2C-Authentikation mit dem CV-Zertifikat bestimmte, von der über das Zugriffsprofil nachgewiesenen Rolle abhängende Zugriffsrechte auf die Daten der anderen Chipkarte.

Bei einem Zugriffsprofil für eine ~~Geräteauthentisierung~~ Authentisierung einer Funktionseinheit eines Gerätes weist eine Chipkarte nach einer C2C-Authentikation mit dem CV-Zertifikat gegenüber der anderen Karte nach, dass sie ~~zu einem bestimmten Gerätetyp gehört~~ die zugehörige Funktionseinheit enthält.

Für die Verteilung der CV-Zertifkate auf die einzelnen Chipkarten gilt aktuell das folgende:

- HBAs, SMC-As und SMC-Bs enthalten mehrere CV-Zertifikate. Ein CV-Rollen-Zertifikat mit einem Zugriffsprofil für eine Rollenauthentisierung und ein oder zwei CV-Geräte-Zertifikate mit einem Zugriffsprofil für eine ~~Geräteauthentisierung~~ Authentisierung einer Funktionseinheit.
- eGKs enthalten ein CV-Rollen-Zertifikat mit einem Zugriffsprofil für eine Rollenauthentisierung.

SMC-Ks und SMC-RFIDs enthalten ein oder zwei CV-Geräte-Zertifikate mit einem Zugriffsprofil für eine ~~Geräteauthentisierung~~ Authentisierung einer Funktionseinheit.

[…]

A.3.2 – ~~Geräteauthentisierung~~ Authentisierung einer Funktionseinheit (normativ)

Aktuell werden die Zugriffsprofile 51 – 55 für eine ~~Geräteauthentisierung~~ Authentisierung einer Funktionseinheit unterschieden:

Tabelle 14: Zugriffsprofile für eine ~~Geräteauthentisierung~~ Authentisierung einer Funktionseinheit

Profil	Kodierung	CV-Zertifikate für	Funktionseinheit
51	'33'	SMC-K	Signaturanwendungskomponente (SAK)
52	'34'	SMC-RFID	Komfortmerkmal
53	'35'	HBA	Stapel- und komfortfähige SSEE und Remote-PIN Empfänger
54	'36'	SMC-A	Remote-PIN Sender
		SMC-B	
55	'37'	SMC-B	Remote-PIN Empfänger
		SMC-RFID (optional)	

Anmerkung 1: Es MUSS sichergestellt werden, dass das Zugriffsprofil in einem CV-Zertifikat dem Typ der Chipkarte entspricht.

Anmerkung 2: Die SMC-RFID enthält nur in der Ausprägung mit PIN-Schutz ein CV-Geräte-Zertifikat mit Profil 55 (s.a. [gemSpec_SMC–RFID#8.2]).

B4 – Tabellenverzeichnis

Tabelle 1: Bereits erfasste Eingangsanforderungen 12

Tabelle 2: Schlüsselanforderungen für die Kartengenerationen der Gesundheitstelematik 20

Tabelle 2a: Referenzierte Schutzbedarfsfeststellung mit Informationsobjekten (Io) 43

Tabelle 3: Beispiel für einen öffentlichen Schlüssel mit Exponent F4 53

[...]

Tabelle 13: Zugriffsprofile für eine Rollenauthentisierung 64

Tabelle 14: Zugriffsprofile für eine ~~Geräteauthentisierung~~ Authentisierung einer Funktionseinheit 65

~~B6 - Klärungsbedarf~~

~~Kap.~~	~~Offener Punkt~~	~~Zuständig~~
~~0~~	~~Es MUSS noch geklärt werden, ob der Karteninhaber~~	~~SPE/ZD~~

~~Kap.~~	~~Offener Punkt~~	~~Zuständig~~
	~~einer SMC-K bzw. einer SMC-RFID den Verlust dieser Chipkarten melden muss. Falls ja MUSS geklärt werden, wo dies gemeldet werden soll~~	~~SPE/DI~~