SRQ - Specification Related Question

SRQ-ID: 1203

Betrifft:

Themenkreis	PKI und Zertifikate
Schlagwort	
zu Dokument / Datei (evtl. ersetzt SRQ)	[gemPKI_CVCGK], ersetzt SRQ 0912
Version	1.4.0
Bezug (Kap., Abschnitt, Tab., Abb.)	3, 4.1.1, 4.1.2, 4.2.3, 4.2.4, 4.2.5, 4.3.1, 4.4, 4.4.2, 4.6

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

Frage:

Welche Anpassungen in dem Dokument ergeben sich aus dem Sicherheitsgutachten und notwendigen Aktualisierungen?

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		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:

- In der Tabelle der Eingangsanforderungen wurde eine bestehende Anforderung zum Schlüsselgebrauch durch eine neue ersetzt (Kapitel 3)
- Die Beispiele zu den Zugriffsprofilen wurden an neue Regelungen angepasst (Abschnitt 4.1.1)
- Ersetzung des Begriffs „Produktion“ bzw. „Kartenproduktion“ durch „Personalisierung“ bzw. „Kartenpersonalisierung“ (Abschnitte 4.1.2 und 4.4)
- sprachliche Präzisierung zu „Zugriffsprofil“ und Präzisierung bzgl. Inhalt des Sicherheitskonzepts (Abschnitt 4.1.2)
- sprachliche Präzisierung bzgl. „Zugriffsprofil einer Funktionseinheit“ (Abschnitt 4.1.2)
- Präzisierung bzgl. Berücksichtigung der Verwendung von Schlüsseln und Zugriffsprofilen im Sicherheitskonzept (Abschnitt 4.1.2)
- Aussagen zur Interoperabilität zwischen Kartengenerationen wurden angepasst (Abschnitt 4.2.3)
- Die Behandlung für den Fall einer Kompromittierung des Schlüsselpaares einer Root-CA und CA der zweiten Ebene wurde angepasst. (Abschnitt 4.2.4)
- Die Vorgaben für die Gültigkeitsdauer und eine mögliche Sperrung eines CV-Zertifikats wurde angepasst. (Abschnitt 4.2.5)
- Anforderung zur Protokollierung des nicht erfolgreichen Einzugs von Chipkarten nach Ablauf der Gültigkeitsdauer wurde aufgenommen (Abschnitt 4.2.5)
- Präzisierung der Beschreibung der Schlüsselgenerierung (Abschnitt 4.3.1)
- Die Tabelle „Schutzbedarf“ wurde angepasst: Wegfall der Aufwandsschätzung, Präzisierung der Maßnahmen zu „Vertraulichkeit der privaten Root- und CA-Schlüssel“ und zu „Verfügbarkeit der privaten Root-Schlüssel“ (Abschnitt 4.4.1 , Tabelle 3)
- Korrektur der Aussage bzgl. Schutzbedarf für Verfügbarkeit des privaten Root-Schlüssels in [gemSiKo] (Abschnitt 4.4.1)
- sprachliche Präzisierung bzgl. Protokollierung der Erstellung von CV-Zertifikaten (Abschnitt 4.4.1)
- Präzisierung der Vorgaben bzgl. Erzeugen des Backup-HSMs (Klonen und Vier-Augen-Prinzip), eine der beiden Varianten MUSS gewählt werden (Abschnitt 4.4.2)
- Änderung der Vorgabe zum Widerruf einer Registrierung durch gematik (Abschnitt 4.4.2)
- Anforderung zur Sicherstellung der Authentizität des öffentlichen Schlüssels der CVC-Root-CA vor dessen Verwendung aufgenommen (Abschnitt 4.4.2)

- Anforderung zur Nutzung des privaten Schlüssels der CVC-Root-CA aufgenommen (Abschnitt 4.4.2)
- Ergänzung der Vorgabe, dass die CA nur für die für sie zugelassenen Endnutzer-Zertifikatstypen ausstellungsberechtigt ist. (Abschnitt 4.4.3)
- Ergänzung der Vorgabe zur Weiternutzung des privaten (Sub-)CVC-CA Schlüssels nach Neugenerierung und im Falle des Widerrufs einer Registrierung: bestehender Schlüssel darf nicht mehr genutzt werden. (Abschnitt 4.4.3)
- Die Verwendungsszenarien von Test-CV-Zertifikaten wurden angepasst (Abschnitt 4.6)

---

3. Anforderungen

[…]

Tabelle 1: Bereits erfasste Eingangsanforderungen

Quelle	Anforderungs-nummer	Anforderungs-level	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 folgenden Unterscheidungsmerkmalen zur Verfügung stellen: … - Card-verifiable-Certificate (CVC, CV-Zertifikat) und CVC-Root …
…			
AM	A_01998	MUSS	Die SMC MUSS ein zweites CV-Zertifikat mit Profil xx zur Geräteauthentisierung enthalten. Dieses CV-Zertifikat MUSS ohne PIN-Eingabe in allen SE#s nutzbar sein. Hierdurch wird eine Trennung von Rollen- (mit Freischaltung) und Geräteauthentisierung (ohne Freischaltung) erreicht

Quelle	Anforderungsnummer	Anforderungslevel	Beschreibung
gemSiKo#B 4.5.3	A_02785	MUSS	Nicht mehr gültige private CVC-Schlüssel MÜSSEN dauerhaft und nachweislich vom weiteren Gebrauch ausgeschlossen werden.

4.1 CV-Zertifikate und ihr Einsatz

4.1.1 Funktion von CV-Zertifikaten

[…]

Beispiele:

- Ein HBA eines Arztes enthält ein CV-Rollen-Zertifikat mit dem Zugriffsprofil 2. Wird dieses CV-Rollen-Zertifikat im Rahmen einer C2C-Authentisierung zwischen dem HBA und einer eGK eingesetzt, erhält der Arzt das Recht, eine eVerordnung in die eGK zu schreiben.
- ~~Ein HBA~~ Eine SMC-B enthält ein CV-Geräte-Zertifikat mit einem Zugriffsprofil 55. Wird dieses CV-Geräte-Zertifikat im Rahmen einer C2C-Authentisierung zwischen ~~dem HBA~~ der SMC-B und einer SMC-A eingesetzt, so kann die SMC-A danach eine PIN (kryptographisch abgesichert) an ~~den HBA~~ die SMC-B senden, da die Funktionseinheit "Empfangen einer Remote-PIN" ~~des HBA~~ der SMC-B authentisiert wurde.
- Ein HBA enthält ein CV-Geräte-Zertifikat mit dem Zugriffsprofil 53. Wird dieses CV-Geräte-Zertifikat im Rahmen einer C2C-Authentisierung zwischen dem HBA und einer SMC-K eingesetzt, so kann die SMC-K danach Daten zum Signieren im Rahmen der Stapel- und Komfortsignatur (kryptographisch abgesichert) an den HBA senden, da die Funktionseinheit "~~Empfangen der DTBS für Stapel- und Komfortsignatur~~ Stapel- und komfortfähige SSEE" des HBA authentisiert wurde.

Die aktuell bei CV-Zertifikaten unterschiedenen Zugriffsprofile und ihre Verteilung auf die verschiednen Chipkarten der Telematikinfrastruktur wird in [gemPKI_Reg#A.3] beschrieben.

4.1.2 Personalisierung der CV-Zertifikate

Die für eine Chipkarte benötigten CV-Zertifikate werden durch eine CA generiert. Bei der Kartenpersonalisierung MÜSSEN dann für die C2C-Authentisierung die folgenden Daten in eine Chipkarte (eGK, HBA, SMC) eingebracht werden:

[…]

Eine CA für das Erzeugen von CV-Zertifikaten kann durch verschiedene Organisationen betrieben werden (siehe Abschnitt 4.2.2). Die Festlegung der notwendigen Regelungen für die Zusammenarbeit zwischen der CA, die das CV-Zertifikat erzeugt und dem

eigentlichen Kartenproduzenten sind nicht Bestandteil dieses Grobkonzepts. Es MÜSSEN aber in jedem Fall die folgenden Punkte erfüllt werden:

- Jede Chipkarte (eGK, HBA bzw. SMC) MUSS (mindestens) ein individuelles CV-Schlüsselpaar haben, d. h. die Personalisierung mehrerer Chipkarten mit einem gemeinsamen Schlüssel ist aus Sicherheitsgründen nicht zulässig.
- Benötigt eine Chipkarte mehrere CV-Zertifikate, da sie mit verschiedenen Zugriffsprofilen C2C-Authentisierungen durchführen muss (z. B. ein HBA), MUSS sie für jedes CV-Zertifikat ein eigenes Schlüsselpaar haben. Das Erzeugen von verschiedenen CV-Zertifikaten (mit unterschiedlichen Zugriffsprofilen) über den gleichen öffentlichen Schlüssel ist nicht zulässig.
- Bei der ~~Produktion~~ Personalisierung eines HBA MUSS sichergestellt sein, dass die einzubringenden CV-Zertifikate entweder genau das Zugriffsprofil enthalten, das zu der Rolle der Leistungserbringer-Gruppe (z. B. Arzt, Apotheker, etc.) gehört, für die der HBA produziert wird, oder das Zugriffsprofil, das zu einer Funktionseinheit gehört, die (als Kartenanwendung) in einem HBA enthalten ist.
- Bei der ~~Produktion~~ Personalisierung einer SMC MUSS sichergestellt werden, dass die einzubringenden CV-Zertifikate entweder genau das Zugriffsprofil enthalten, das zu der Rolle der entsprechenden Einrichtung gehört, für die die SMC produziert wird, oder das Zugriffsprofil, das zu einer Funktionseinheit gehört, die (als Kartenanwendung) in der SMC enthalten ist.
- Bei der ~~Produktion~~ Personalisierung einer eGK MUSS sichergestellt werden, dass das einzubringende CV-Zertifikat genau das Zugriffsprofil 0 enthält, über das keinerlei Rechte vergeben werden.

Die Sicherstellung dieser Anforderungen liegt in der Verantwortung der CA (in Zusammenarbeit mit dem Kartenherausgeber und dem Kartenhersteller), die CV-Zertifikate für Chipkarten ausstellt. Die Verwendung von individuellen Schlüsselpaaren und der korrekten Zugriffsprofile beim Einbringen der CV-Zertifikate auf der Chipkarte MUSS in dem Sicherheitskonzept der CVC-CA beschrieben werden. Siehe hierzu auch die entsprechenden Ausführungen in [gemPKI_Reg].

4.2.3 Interoperabilität zwischen Kartengenerationen

Aktuell werden für die Chipkarten der Telematikinfrastruktur die drei Generationen G0, G1 und G2 unterschieden. Bezüglich der C2C-Authentisierung 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: Aktuelle Vorgaben für die verschiedenen Kartengenerationen

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 (aus technischen Gründen) keine direkte C2C-Authentisierung erfolgreich durchgeführt werden, falls diese dabei Schlüssel unterschiedlicher Länge oder unterschiedliche Algorithmen einsetzen.

[…]

4.2.4 Schlüsselversionen bei Root-CA und CAs

Root-CA und CAs der zweiten Ebene setzen (jeweils) für das Ausstellen von CV-Zertifikaten ein Schlüsselpaar ein, […]

[…]

Im Falle einer Kompromittierung eines Schlüsselpaares ist ein Versionswechsel als alleinige Maßnahme nicht ausreichend. Eine Abschätzung der Auswirkungen einer Kompromittierung eines Schlüsselpaares sowie die daraus folgenden Notfallprozesse müssen in einer Risikoanalyse und Notfallplanung in einem gesonderten Dokument behandelt werden. Diese sind nicht Bestandteil des vorliegenden Grobkonzeptes.

[…]

4.2.5 Lebenszyklus eines CV-Zertifikats

Der Lebenszyklus eines CV-Zertifikats wird in [gemPKI_Reg#4.8] beschrieben. Bezüglich der Lebensdauer und einer möglichen Sperrung eines CV-Zertifikats gelten dabei die folgenden Vorgaben:

- CV-Zertifikate haben nach ihrer Generierung theoretisch eine unbegrenzte Gültigkeit~~ 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 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 Kartenherausgeber vorgegeben. Ein entsprechender Einzug einer Chipkarte durch den Kartenherausgeber MUSS durch diesen protokolliert werden. Der Kartenherausgeber MUSS auch die Fälle dokumentieren, in denen der Einzug von Chipkarten, deren Gültigkeitsdauer abgelaufen ist, nicht möglich war. Diese Information MUSS mindestens in das ISMS (Informationssicherheitsmanagementsystem) des Kartenherausgebers

einfließen und dort behandelt werden. Zum Zwecke einer Risikobewertung und ggf. zu ergreifenden mitigierenden Maßnahmen MÜSSEN die Informationen über nicht eingezogene Chipkarten regelmäßig ausgewertet werden. 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.

- Falls die zu den CV-Zertifikaten gehörenden Schlüsselpaare ihre Gültigkeit verlieren, gilt das gleiche wie bei Ablauf der Gültigkeit der Chipkarte.
- CV-Zertifikate können (nach aktuellem Stand 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.

Es muss noch geklärt werden, ob ggf. doch ein Sperren einzelner CV-Zertifikate in der PKI umgesetzt werden soll, und falls ja, wie diesen Funktion umgesetzt werden soll.

4.3.1 Generierung eines neuen Schlüsselpaares für die Root-CA

[…]

Teilprozesse:

1a) Generierung des neuen Schlüsselpaares

Das neue Schlüsselpaar MUSS intern in dem verwendeten HSM erzeugt werden.

1b) […]

4.4 Grundlagen für die Sicherheit

Die Sicherheit der PKI für CV-Zertifikate ist für die Sicherheit des Gesamtsystems von entscheidender Bedeutung. Durch das Ausstellen von CV-Zertifikaten ermöglicht eine CA der zweiten Ebene (in Zusammenarbeit mit einem Kartenhersteller und bei Vorhandensein der sonstigen für die ~~Produktion~~ Personalisierung benötigten Daten) die Herstellung […]

4.4.1 Sicherheitsanforderungen und Schutzbedarf

[…]

Tabelle 3 – Schutzbedarf

Sicherheitsziel	Schutzbedarf	Erläuterung	~~Aufwand~~Maßnahmen
Vertraulichkeit der privaten Root- und CA-Schlüssel	sehr hoch [gemSiKo#C2.87] [gemSiKo#C2.89]	Eine Kompromittierung hätte zur Folge, dass falsche CV-Zertifikate ausgestellt werden können.	~~mittel:~~ Ein gemäß den Forderungen der gematik zertifiziertes HSM oder eine zertifizierte Chipkarte kann den Schutzbedarf abdecken
Nur autorisierte Nutzung der privaten Root- und CA-Schlüssel	sehr hoch	Nicht autorisierte Nutzung hätte zur Folge, dass falsche CV-Zertifikate ausgestellt werden können.	~~hoch:~~ Rollen und Nutzungskonzept für die CA. Zugriff auf HSM durch Chipkarte bzw. PIN absichern.
Verfügbarkeit der privaten Root-Schlüssel	hoch [gemSiKo#C2.87] (siehe Anmerkung nach der Tabelle)	Es könnten sonst keine weiteren CV-Zertifikate für CAs der zweiten Ebene ausgestellt werden.	~~mittel:~~ Backup HSM für die Root-CA, verschlüsselte Aufteilung Schlüssel-Backup auf Chipkarten oder zweites HSM mit eigenem Schlüsselpaar mit Cross CV-Zertifikaten.
Authentizität des öffentlichen Schlüssels der Root-CA	sehr hoch [gemSiKo#C2.88]	Dieser Schlüssel muss in jede Chipkarte (eGK, HBA, SMC) eingebracht werden. Karten mit falschem Schlüssel können nicht korrekt verwendet werden.	~~Mittel:~~ Verteilung über zwei Wege, z. B. über Internet/Server und Fingerprint über Briefpost.
Authentizität des öffentlichen Schlüssels der CAs der zweiten Ebene	sehr hoch [gemSiKo#C2.90]	Wird die Authentizität nicht überprüft, kann eine nicht registrierte CA ein CV-Zertifikat erhalten und sich so als CA der zweiten Ebene ausgeben.	~~Mittel:~~ Übermittlung über zwei getrennt Wege, Aufwand nicht hoch da die Anzahl der CAs der zweiten Ebene gering ist.
Nachvollziehbarkeit (Revisionssicherheit) Root-CA (gematik)	sehr hoch [gemSiKo#C2.90]	Die Root-PKI muss registrieren, welcher Dienstleister welches CA-CV-Zertifikat bekommen hat.	~~mittel:~~ Organisatorische Aufgabe, geringer Anzahl von Personalisierern, Protokollierung aller ausgestellter CA-CV-Zertifikate.
Nachvollziehbarkeit (Revisionssicherheit) CA für HBA/SMC (Dienstleister)	sehr hoch [gemSiKo#C2.27] [gemSiKo#C2.64] [gemSiKo#C2.68]	Die CA muss protokollieren, welches CV-Zertifikat in welcher Karte (HBA/SMC) vorhanden ist. Der Kartenherausgeber	~~Hoch:~~ Protokollierung aller ausgestellter CV-Zertifikate mit einem Zugriffsprofil ungleich 0.

Sicherheitsziel	Schutzbedarf	Erläuterung	~~Aufwand~~Maßnahmen
		muss registrieren, welcher Karteninhaber welche Karte (HBA/ SMC) erhalten hat.	
Nachvollziehbarkeit (Revisionssicherheit) CA für eGKs (Dienstleister)	sehr hoch [gemSiKo#C2.24]	Eine Registrierung oder Verwaltung, welcher Versicherter welches CV-Zertifikat bekommen hat, ist nicht erforderlich.	~~Niedrig:~~ Protokollierung der Anzahl der erzeugten CV-Zertifikate mit einem Zugriffsprofil gleich 0.

Anmerkung: ~~Aktuell ist für die Verfügbarkeit des privaten Root-Schlüssels in [gemSiKo#C2.87] nur der Schutzbedarf niedrig angegeben. An dieser Stelle wird das Sicherheitskonzept noch entsprechend überarbeitet werden.~~ Die Verfügbarkeit des privaten Root-Schlüssels ist gemäß des Informationsschutzobjektes „Io122“ in [gemSiKo#C2.87] mindestens hoch. Der private Schlüssel der Root-CA MUSS mit hoher Zuverlässigkeit wiederhergestellt werden können. Ansonsten könnte bei einem Verlust des Root-Schlüssels die Situation eintreten, dass aktuell im Feld befindliche Chipkarten mit zukünftig neu produzierten Chipkarten keine C2C-Authentisierung mehr durchführen können.

Es MUSS sichergestellt werden, dass eine CA ~~MUSS grundsätzlich~~ die Erstellung aller solcher CV-Zertifikate revisionssicher protokolliert, die in dem Zugriffsprofil (Profil Byte im Feld CHA des CV-Zertifikats) einen Wert ungleich 0 haben. Dies gilt unabhängig davon, ob die CA als "CA für HBA/SMC“ oder als "CA für eGK“ arbeitet [gemSiKo# B4.5.3].

[…]

4.4.2 Sicherheit bei der Root-CA

[…]

Für die Realisierung des benötigten Backup-HSMs MUSS ~~KANN~~ dabei eine der beiden folgenden Alternativen gewählt werden:

- Das Backup-HSM enthält das gleiche Schlüsselpaar wie das eigentliche HSM. In diesem Fall MUSS zwischen HSM und Backup-HSM ein kryptographisch gesicherter Transportkanal hergestellt werden, um den privaten Schlüssel aus dem HSM verschlüsselt zu exportieren und in das Backup-HSM zu importieren. Vertraulichkeit und Integrität des privaten Schlüssels MÜSSEN dabei zu jedem Zeitpunkt gewährleistet sein. Bei dem Erzeugen des Backup-HSMs MÜSSEN die Vorgaben für das Klonen und die Umsetzung des Vier-Augen-Prinzips aus [gemSiKo#B4.5] eingehalten werden.

- Das Backup-HSM enthält ein anderes Schlüsselpaar wie das eigentliche HSM. In diesem fall MUSS das Schlüsselpaar in dem Backup-HSM sicher generiert werden. Nach dem Generieren des Schlüsselpaares MÜSSEN unmittelbar die beiden Cross-CV-Zertifikate zwischen dem Schlüsselpaar in dem HSM und dem Schlüsselpaar in dem Backup-HSM erzeugt werden. Die Verfügbarkeit der Cross-CV-Zertifikate MUSS gewährleistet sein. In diesem

Fall entspricht der Übergang von dem HSM zu dem Backup-HSM einem Wechsel der Root-Version.

Organisatorische Vorgaben (für gematik und technischer Betreiber):

- Die gematik MUSS CAs der zweiten Ebene registrieren ([gemPKI_Reg#5]).
- Die gematik ~~KANN~~ MUSS imstande sein, eine Registrierung einer CA der zweiten Ebene ggf. zu widerrufen ([gemPKI_Reg#5]).
- Die gematik MUSS dem technischen Betreiber der Root-CA immer eine aktuelle Liste der registrierten CAs der zweiten Ebene zur Verfügung stellen.
- Die Root-CA DARF ein CV-Zertifikat für eine CA NICHT ausstellen, falls diese nicht aktuell durch die gematik registriert ist.
- Der Schutzbedarf bezüglich des Schutzziels „Authentizität“ des öffentlichen Schlüssels der CVC-Root-CA ist „sehr hoch“. Der Betreiber der CVC-Root-CA MUSS die Authentizität des öffentlichen Schlüssels der CA bei der Veröffentlichung für andere Akteure (z.B. Betreiber CVC-CA der zweiten Ebene) durch die durchgängige Umsetzung des 4-Augen-Prinzips sicherstellen. Die Umsetzung MUSS im Sicherheitskonzept des Betreibers der CVC-Root-CA beschrieben sein.
- Der private Schlüssel der CVC-Root-CA DARF NICHT für andere Zwecke als die Erstellung von Zertifikaten für (Sub-)CVC-CAs verwendet werden ([gemSiKo#AnhF], SP_KEY_USE_1).

4.4.3 Sicherheit bei einer CA der zweiten Ebene

[…]

Für eine CA der zweiten Ebene MUSS in einem Sicherheitskonzept dargestellt werden, wie die Vorgaben der gematik für den Mindeststandard der Sicherheit umgesetzt werden. Eine CA der zweiten Ebene MUSS sich bei der gematik registrieren lassen. Im Rahmen dieser Registrierung MUSS die Einhaltung dieser Vorgaben durch ein Sicherheitsgutachten nachgewiesen werden.

Es MUSS sicher gestellt werden, dass die CA der zweiten Ebene nur Enduser-Zertifikate der Typen ausgibt, für die die CA zugelassen ist.

Es DARF NICHT möglich sein, den privaten Schlüssel weiterhin zu verwenden, falls für die Aufgaben eines (Sub-)CVC-CA Schlüsselpaars ein neues Schlüsselpaar generiert wurde oder falls die Registrierung der CVC-CA durch die gematik widerrufen wurde [gemSiKo_AnhB#A_04269]. Die Mindestanforderungen an die Sicherheit einer CA der zweiten Ebene werden in [gemPKI_Reg#6] beschrieben.

Text von [gemSiKo_AnhB#A_04269]: „Es DARF NICHT mehr möglich sein, den privaten Schlüssel weiterhin zu verwenden, falls für die Aufgaben eines (Sub-)CVC-CA Schlüsselpaars ein neues Schlüsselpaar generiert wurde oder falls die Registrierung der CVC-CA durch die gematik widerrufen wurde.“

4.6 Unterscheidung Testbetrieb – Produktivbetrieb

[…]

Test-CV-Zertifikate werden nicht nur für eine Testphase während der Einführung des Systems benötigt. Sie werden vielmehr auch zu späteren Zeitpunkten benötigt, falls z. B.

- eine neue CA ihren Betrieb als CA der zweiten Ebene aufnehmen und testen möchte,
- ein neuer Kartenhersteller seinen Betrieb aufnehmen möchte und dazu zunächst Musterkarten produzieren möchte,
- ~~Terminalhersteller~~ Hersteller von Kartenterminals, Konnektoren und Primärsystemen für das Austesten neuer Produkte Musterkarten benötigen.