gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

PKI für CV-Zertifikate

Grobkonzept

Version:	1.4.0
Stand:	19.03.2008
Status:	freigegeben

Dokumentinformationen

Änderungen zur Version 1.2.0

Das Dokument wurde vollständig überarbeitet. Im Einzelnen wurden u. a. folgenden Änderungen/Ergänzungen vorgenommen:

- Kapitel 3 wurde für die Darstellung der Anforderungen vorbereitet. Die Anforderungen selber müssen noch mit dem Anforderungsmanagement abgestimmt werden. Aktuell wurden in Kapitel 3 alle die Anforderungen des AM aufgenommen, die im weitesten Sinne relevant für CV-Zertifikate sind.
- Die neuen Gegebenheiten bei den Karten der Generation 1 wurden berücksichtigt.
- Ein kurzer Abschnitt zu dem Thema „Interoperabilität zwischen verschiedenen Kartengenerationen“ wurde eingefügt.
- Der in der Vorgängerversion verwendete Begriff Generation wurde durchgängig durch den Begriff Root-Version ersetzt.
- Bei den Sicherheitsanforderungen wurden an den relevanten Stellen auf entsprechende Vorgaben aus dem gematik-Sicherheitskonzept verwiesen.
- Die Beschreibung der Mindestanforderungen an eine CVC-CA der zweiten Ebene wurde entfernt und durch eine Referenz auf [gemPKI_Reg#6] ersetzt.
- Der Abschnitt „Sicherheitsanforderungen und Schutzbedarf“ wurde in den Abschnitt „Grundlagen der Sicherheit“ verschoben.
- Die Unterscheidung zwischen CV-Rollen-Zertifikaten und CV-Geräte-Zertifikaten sowie die Unterscheidung zwischen Rollenauthentisierung und Geräteauthentisierung wurden eingeführt.
- Ein Abschnitt über den Lebenszyklus der CV-Zertifikate wurde eingefügt.
- In dem Abschnitt über Produktiv- und Testbetrieb wurde ein Hinweis auf die Nutzung der CV-Zertifikate in Produktiv-, Test- und Musterkarten eingefügt.
- Liste der Referenzen wurde ergänzt.
- Liste der offenen Punkte wurde ergänzt.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemPKI_CVCGK]	gematik (19.03.2008): Einführung der Gesundheitskarte - PKI für die CV-Zertifikate: Grobkonzept Version 1.4.0

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	10.11.05		Basisversion zur internen und externen Kommentierung vorgelegt	gematik, IQS
0.0.2	20.12.05		Einarbeitung des CVC-Konzeptes V0.7b	BÄK
0.0.3	21.12.05		Überarbeitung	BÄK
0.1	30.01.06		Überarbeitung/Ergänzung	gematik, AG3
0.1.1	14.02.06		Überarbeitung nach Kommentierung QS	gematik, AG3
1.0.0	13.04.06		Überarbeitung nach Fertigstellung Registrierungsdokument	gematik
1.1.0	15.06.06		Anmerkungen QS DAK,KBV eingearbeitet „geklonte HSM“ neu eingeführt Hinweise auf Aufbau Root-CA gestrichen Begriff HPC durch HBA/SMC ersetzt.	gematik
1.1.1	23.08.07	3.1.3	Klarstellung Trennung Verantwortlichkeit Betreiber CA und Kartenherausgeber	gematik, AG8
1.2.0	27.08.07		freigegeben	gematik
1.2.1	27.02.08		Vollständige Überarbeitung aufgrund der Generationen 0,1,2 bei eGKs und neuer Sicherheitsmodule SMC-K und SMC-RFID	SPE/ZD
1.3.0	29.02.08		freigegeben	gematik
1.3.2	17.03.08		Einarbeitung Kommentare der gematik-QS	SPE/ZD
1.4.0	19.03.08		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Chipkarten der Telematikinfrastruktur (eGK, HBA, SMC) enthalten für eine direkte gegenseitige Card-to-Card-Authentisierung (kurz: C2C-Authentisierung) entsprechende Schlüsselpaare und zugehörige CV-Zertifikate. Im Rahmen einer C2C-Authentisierung weist eine Chipkarte ihre Echtheit gegenüber der anderen Chipkarte nach. Zusätzlich können dabei ein sicherer Kanal zwischen den beteiligten Chipkarten aufgebaut werden, bestimmte Zugriffsrechte auf Daten in einer der beteiligten Chipkarten erlangt werden und/oder die Ausführung bestimmter Funktionen durch eine der beteiligten Chipkarte freigegeben werden.

CV-Zertifikate werden gemäß der Kartenspezifikationen verwendet, weil Chipkarten aufgrund ihrer Leistungsfähigkeit zurzeit ausschließlich dieses Zertifikatsformat intern verarbeiten können. Es handelt sich bei der C2C-Authentisierung um eine Offline-Authentisierung, die durch Konnektor und Kartenterminal entsprechend unterstützt werden muss.

Dieses Grobkonzept gibt einen Überblick über den Einsatz der CV-Zertifikate in der Telematikinfrastruktur und über die PKI, die für das Erzeugen dieser CV-Zertifikate betrieben wird. Im Gegensatz zu der PKI für X.509-Zertifikate ist die PKI für CV-Zertifikate dabei eine hierarchische PKI mit einer zentralen Root CA. Die Root CA wird dabei in der Verantwortung und im Auftrage der gematik betrieben.

Das vorliegende Dokument muss im Zusammenhang mit dem Dokument [gemPKI_Reg] betrachtet werden. Während dieses Dokument die Grundlagen und Zusammenhänge grob skizziert, enthält das Dokument [gemPKI_Reg] die konkreten technischen Anforderungen und Vorgaben für den Betrieb einer CA für das Erzeugen von CV-Zertifikaten.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Dieses Dokument enthält in Kapitel 4 einen Überblick über den Einsatz der CV-Zertifkate in den Chipkarten der Telematikinfrastruktur und deren Erzeugung im Rahmen der gesondert betriebenen PKI für CV-Zertifikate. Es werden insbesondere die Grundlagen für Aufbau und Betrieb der PKI zusammengestellt. Die konkreten technischen Vorgaben zu diesem Thema sind nicht in diesem Dokument enthalten, diese werden vielmehr in [gemPKI_Reg] beschrieben.

2.2 Zielgruppe

Dieses Dokument richtet sich an alle, die einen Überblick über den Einsatz der CV-Zertifikate in den Chipkarten der Telematikinfrastruktur und deren Erzeugung im Rahmen der PKI für CV-Zertifikate benötigen. Dazu gehören Kartenherausgeber, -hersteller und –personalisierer der Chipkarten der Telematikinfrastruktur (eGK, HBA, SMC) sowie Betreiber einer CA für das Erzeugen von CV-Zertifikaten.

2.3 Geltungsbereich

Die in diesem Dokument enthaltenen Vorgaben sind verbindlich für Kartenherausgeber, -hersteller und –personalisierer von eGKs, HBAs und SMCs sowie für Betreiber einer CA, sofern sie mit dieser CA CV-Zertifikate für eGKs, HBAs oder SMCs erzeugen.

2.4 Arbeitsgrundlagen

Die wesentliche Grundlage für die Vorgaben dieses Lastenheftes bilden die folgenden Dokumente:

- Spezifikation der eGK [gemSpec_eGK_P1], [gemSpec_eGK_P2]
- Spezifikation der HBA und SMC [HPC-P1], [HPC-P2], [HPC-P3]

Bezüglich der Sicherheitsanforderungen und der zu verwendenden Algorithmen basiert dieses Lastenheft auf den folgenden Dokumenten:

- Übergreifendes Sicherheitskonzept der TI [gemSiKo]
- Vorgaben für die Verwendung kryptographischer Algorithmen [gemSpec_Krypt]

2.5 Abgrenzung des Dokumentes

Das Sicherheitskonzept der Telematikinfrastruktur [gemSiKo] enthält übergreifende Vorgaben für die Sicherheitsanforderungen, die für das vorliegende Dokument normativ sind. Die Beschreibungen in diesem Dokument sind daher als Konkretisierungen zu verstehen, wie diese übergreifenden Sicherheitsanforderungen umgesetzt und durch welche konkreten Sicherheitsmaßnahmen diese Anforderungen erfüllt werden bzw. welche Umgebungsanforderungen von anderen Diensten oder dem Betreiber zu erfüllen sind.

Die bei einer C2C-Authentisierung zum Einsatz kommenden Algorithmen und die Längen der beteiligten Schlüssel werden nicht durch dieses Dokument vorgegeben. Diese werden vielmehr durch die Spezifikationen [gemSpec_Krypt] und [gemSpec_eGK_P1] unter Berücksichtigung der Vorgaben aus [gemSiKo] festgelegt.

Dieses Dokument gibt einen Überblick über den Einsatz von CV-Zertifikaten und ihrer Erzeugung im Rahmen einer PKI für CV-Zertifikate. Die konkreten technischen Details sind in dem Dokument [gemPKI_Reg] enthalten.

Aktuell werden für die Chipkarten der Telematikinfrastruktur drei Generationen G0, G1 und G2 unterschieden. Für jede Kartengeneration wird eine eigene CVC-PKI aufgebaut. Die Vorgaben in der aktuellen Version dieses Dokuments gelten dabei zunächst nur für die CVC-PKI für die Kartengeneration G1. Für die CVC-PKI für die Kartengeneration G0 gelten weiterhin die Vorgaben aus der Version 1.2.0 vom 27.08.2007 dieses Dokuments.

2.6 Methodik

2.6.1 Verwendung von Schlüsselworten

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem RFC 2119 [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

- **MUSS** bedeutet, dass es sich um eine absolutgültige und normative Festlegung bzw. Anforderung handelt.
- **DARF NICHT** bezeichnet den absolutgültigen und normativen Ausschluss einer Eigenschaft.
- **SOLL** beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **SOLL NICHT** kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **KANN** bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

2.6.2 Hinweis auf offene Punkte

Auf offene Punkte wird durch einen Text in nachfolgendem Format hingewiesen:

Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

3 Anforderungen

1) Die Anforderungen müssen noch mit dem Anforderungsmanagement abgestimmt werden. Das Kapitel wird in einer späteren Version des Dokumentes entsprechend überarbeitet.
2) Der Umgang mit den Ausgangsanforderungen muss gemäß den Vorgaben aus dem Handbuch Standards und Konventionen überarbeitet werden.

Die Notwendigkeit für eine PKI für die benötigten CV-Zertifikate für die Chipkarten ergibt sich aus der Gesamtarchitektur. Die gematik muss die Interoperabilität zwischen dieser PKI und den sie nutzenden Komponenten/Prozessen sicherstellen.

Die folgende Tabelle enthält die entsprechenden, für CV-Zertifikate relevanten Eingangsanforderungen, wie sie aktuell bereits identifiziert werden können:

Tabelle 1: Bereits erfasste Eingangsanforderungen

Quelle	Anforderungs-nummer	Anforderungs-level	Beschreibung
AM	A_00124	MUSS	Die als eGK eingesetzten Chipkarten MÜSSEN die Authentifizierung und Autorisierung der Zugriffe von berechtigten Heilberuflern bzw. deren Institutionen auf der Basis von CVC (Card-Verifyable-Certificates) selbst durchführen.
AM	A_00749	MUSS	Die eGK MUSS über X.509- und CVC-Authentifizierungszertifikate gesichert werden
AM	A_00802	MUSS	Es MUSS für HBA und eGK eine PKI zur Ausstellung von CV-Zertifikaten betrieben werden.
AM	A_00820	MUSS	Der Entstehungs- und Löschprozess eines konkreten CVC-Zertifikates in der TI MUSS einer durchführenden Person eindeutig zuordenbar sein
AM	A_00821	MUSS	Ein CVC-Zertifikat MUSS auf einem Medium gespeichert sein, das ausreichend robust ist, damit sie mindestens für ihren Gültigkeitszeitraum nutzbar sind
AM	A_00822	MUSS	Ein CVC-Zertifikat MUSS am zentralen Speicherort vor Veränderung geschützt werden
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)

Quelle	Anforderungsnummer	Anforderungslevel	Beschreibung
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_01847	MUSS	Es MUSS ein Profil 8 erstellt werden, welches VSD (frei auslesbare und GVD) über CVC lesen kann
AM	A_01868	MUSS	Jede SMC MUSS die Fähigkeit besitzen, sowohl SHA-256 als auch SHA-1 in der Karte zu rechnen zu können. (Vorgabe der TR 03116. CVC wird auf 2048 bit und SHA-256 umgestellt. …)
AM	A_01871	MUSS	Der HBA MUSS die Fähigkeit besitzen, RSA für CVC mit Schlüssellängen von 2048 bit zu rechnen. (Vorgabe der TR 03116)
AM	A_01888	MUSS	Jede SMC MUSS die Fähigkeit besitzen, RSA für CVC mit Schlüssellängen von 2048 bit zu rechnen. (Vorgabe der TR 03116)
AM	A_01992	MUSS	Das Format der CV-Zertifikate auf dem HBA MUSS dem Format entsprechen, das in der aktuellen - zum Release der HBA-Spezifikation gehörenden - eGK-Spezifikation Teil 1 definiert ist. (Interoperabilität)
AM	A_01993	MUSS	Die Rollenauthentisierung und die Rollenprüfung MÜSSEN beim HBA den Vorgaben in der aktuellen – zum Release der HBA-Spezifikation gehörenden – eGK-Spezifikation Teil 1 entsprechen. (Interoperabilität)
AM	A_01994	MUSS	Der HBA 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. (notwendig zur gegenseitigen Geräteauthentisierung zum Aufbau eines TC)
AM	A_01996	MUSS	Das Format der CV-Zertifikate auf der SMC MUSS dem Format entsprechen, das in der - zum jeweils aktuellen Release gehörenden - eGK-Spezifikation Teil 1 definiert ist. (Interoperabilität)
AM	A_01997	MUSS	Die Rollenauthentisierung und die Rollenprüfung MÜSSEN bei der SMC den Vorgaben in der - zum jeweils aktuellen Release gehörenden - eGK-Spezifikation Teil 1 entsprechen. (Interoperabilität
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

Quelle	Anforderungsnummer	Anforderungslevel	Beschreibung
			Freischaltung) und Geräteauthentisierung (ohne Freischaltung) erreicht

4 Grobkonzept für die PKI für CV-Zertifikate

4.1 CV-Zertifikate und ihr Einsatz

4.1.1 Funktion von CV-Zertifikaten

Chipkarten der Telematikinfrastruktur (eGK, HBA, SMC) enthalten für eine direkte gegenseitige Authentisierung entsprechende Schlüsselpaare und zugehörige CV-Zertifikate. Durch diese so genannte Card-to-Card-Authentisierung (kurz: C2C-Authentisierung) weist eine Chipkarte ihre Echtheit gegenüber der anderen Chipkarte nach. Zusätzlich kann in Abhängigkeit von der konkret durchgeführten C2C-Authentisierung und dem Inhalt der dabei zum Einsatz kommenden CV-Zertifikate noch einer oder mehrere der folgenden Punkte erreicht werden:

- Zwischen den beiden Chipkarten wird ein sicherer Kanal aufgebaut, über den anschließend kryptographisch abgesicherte Daten zwischen den Chipkarten ausgetauscht werden können.
  Beispiel: C2C-Authentisierung zwischen einer SMC-K und einem HBA im Rahmen der Stapel- und Komfortsignatur.

- In einer der Chipkarten werden abhängig von dem CV-Zertifikat der anderen Chipkarte Zugriffe auf bestimmte Daten freigegeben.
  Beispiel: C2C-Authentisierung zwischen einer eGK und einem HBA zum Lesen bzw. Schreiben einer eVerordnung.

- In einer der Chipkarten werden abhängig von dem CV-Zertifikat der anderen Chipkarte bestimmte Funktionalitäten freigegeben.
  Beispiel: C2C-Authentisierung zwischen einem HBA und einer SMC-A zum Freischalten der SMC-A.

CV-Zertifikate können (im Gegensatz zu X.509-Zertifikaten) durch eine Chipkarte intern verifiziert und analysiert werden. Abhängig von dem Inhalt eines, ihr im Rahmen einer C2C-Authentisierung präsentierten CV-Zertifikats einer anderen Chipkarte, entscheidet die verifizierende Chipkarte dann bei ihrer weiteren Arbeit über Zugriffsrechte auf in ihr gespeicherten Daten und/oder über die Ausführbarkeit von Funktionen. CV-Zertifikate und ihr Einsatz bei der C2C-Authentisierung basieren auf der europäischen Norm [14890-1] und [14890-2]. Der Aufbau der CV-Zertifikate für die Chipkarten der Telematikinfrastruktur sowie das Vorgehen bei dem Berechnen bzw. Verifizieren dieser CV-Zertifikate werden durch die Spezifikation der eGK in [gemSpec_eGK_P1#8.1] vorgegeben. Diese Vorgaben werden durch die Spezifikation des HBA und der SMC ([HPC-P1], [HPC-P2], [HPC-P3]) übernommen. Eine kurze Zusammenfassung hierzu findet man in [gemPKI_Reg#A.1].

Neben verschiedenen technischen Parametern enthält ein CV-Zertifikat einer Chipkarte die ICCSN dieser Chipkarte und ein Zugriffsprofil. Bei korrekter Vergabe der ICCSN identifiziert diese die Chipkarte weltweit eindeutig (siehe [gemSpec_eGK_P1#6.2.5]). Über das in einem CV-Zertifikat enthaltene Zugriffsprofil wird festgelegt, welche konkreten Rechte bezüglich der Zugriffe auf Daten oder der Ausführbarkeit weiterer Funktionen in einer Chipkarte nach der C2C-Authentisierung erlangt werden. Dabei wird zwischen

- Zugriffsprofilen für eine Authentisierung einer Rolle und
- Zugriffsprofilen für eine Authentisierung einer Funktionseinheit der Chipkarte

unterschieden.

Begrifflichkeit:

- CV-Zertifikate mit einem Zugriffsprofil für eine Rollenauthentisierung werden auch als CV-Rollen-Zertifikate bezeichnet.
- CV-Zertifikate mit einem Zugriffsprofil für eine Authentisierung einer Funktionseinheit werden auch als CV-Geräte-Zertifikate 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 CV-Geräte-Zertifikate.
- HBAs, SMC-As und SMC-Bs enthalten sowohl ein CV-Rollen-Zertifikat als auch (ggf. mehrere) CV-Geräte-Zertifikate.

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-Authentisierung auf die in der anderen Chipkarte gespeicherten Daten erhält.

Authentisierung einer Funktionseinheit: 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, welche Funktionseinheit diese Chipkarte enthält.

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 enthält ein CV-Geräte-Zertifikat mit einem Zugriffsprofil 55. Wird dieses CV-Geräte-Zertifikat im Rahmen einer C2C-Authentisierung zwischen dem HBA und einer SMC-A eingesetzt, so kann die SMC-A danach eine PIN (kryptographisch abgesichert) an den HBA senden, da die Funktionseinheit "Empfangen einer Remote-PIN" des HBA 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" 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 Kartenproduktion MÜSSEN dann für die C2C-Authentisierung die folgenden Daten in eine Chipkarte (eGK, HBA, SMC) eingebracht werden:

- Ggf. mehrere private Schlüssel der Chipkarte für die C2C-Authentisierung.
- Kartenindividuelle CV-Zertifikate über die zugehörigen öffentlichen Schlüssel.
- CV-Zertifikat der CA, die die kartenindividuellen CV-Zertifikate ausgestellt hat.
- Öffentlicher Schlüssel der Root-CA.

Diese Daten können (nach dem aktuellen Stand der Spezifikation der Chipkarten-Anwendungen) nach der Kartenausgabe (an den Versicherten, Arzt, etc.) nicht mehr nachträglich eingebracht bzw. verändert 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 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 zu einer Funktionseinheit gehört, die (als Kartenanwendung) in einem HBA enthalten ist.
- Bei der Produktion 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 zu einer Funktionseinheit gehört, die (als Kartenanwendung) in der SMC enthalten ist.
- Bei der Produktion 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. Das Vorgehen hierbei muss in dem Sicherheitskonzept der CA beschrieben werden. Siehe hierzu auch die entsprechenden Ausführungen in [gemPKI_Reg].

4.2 Rahmenbedingungen für den Aufbau der PKI

4.2.1 Hierarchie der CV-Zertifikate

Die folgende Abbildung gibt einen schematischen Überblick über die PKI für CV-Zertifikate:

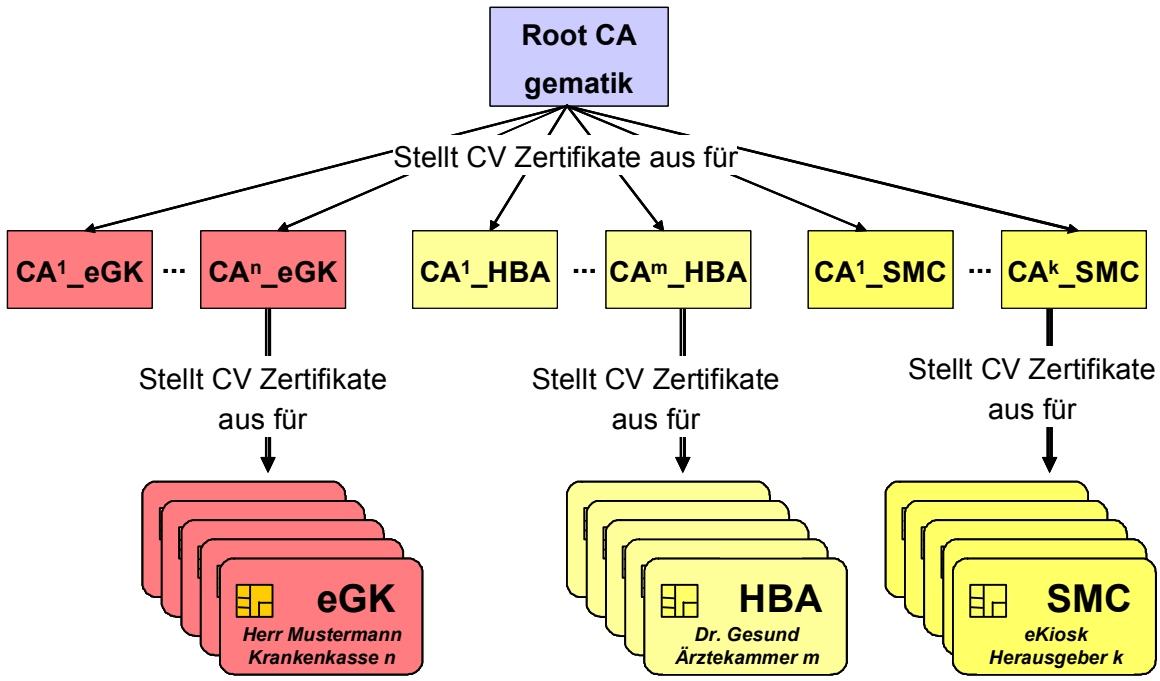

Abbildung 1 – Hierarchie der PKI für CV-Zertifikate

Auf oberster Ebene stellt die Root-CA CV-Zertifikate für die CAs der zweiten Ebene aus. Die eigentlichen CV-Zertifikate über die kartenindividuellen Schlüssel einer Chipkarte (eGK, HBA, SMC) werden dann durch die entsprechende (durch den Kartenherausgeber beauftrage) CA ausgestellt.

Wie in Abschnitt 4.1.1 beschrieben kann eine Chipkarte für die C2C-Authentisierung mehrere private Schlüssel enthalten. Entsprechend gehören dann zu der Chipkarte auch mehrere CV-Zertifikate über die verschiedenen öffentlichen Schlüssel. Die zu einer Chipkarte gehörenden CV-Zertifikate werden jedoch alle durch die gleiche CA der zweiten Ebene erzeugt.

Vorteile der zweistufigen PKI für die CV-Zertifikate sind,

- dass Kostenträger und Leistungserbringer für die CAs in ihrem Verantwortungsbereich (weitestgehend) eigene Vorgaben erstellen können,
- dass Kartenherausgeber für das Erzeugen der CV-Zertifikate für die von ihnen herausgegebenen Chipkarten (eGK, HBA, SMC) eigene CAs betreiben können bzw. dafür geeignete Dienstleister beauftragen können,
- dass durch eine einzige übergeordnete Root-CA mittels Zertifizierung der zugehörigen CAs eine einheitliche PKI für die CV-Zertifikate entsteht.

4.2.2 Registrierung durch die gematik

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

- Kartenpersonalisierer,
- Kartenhersteller,
- Kartenherausgeber,
- ZDAs im Sinne vom SigG

Damit eine Organisation eine CA der zweiten Ebene für das Generieren von CV-Zertifikaten betreiben kann, MUSS diese durch die gematik registriert werden. Im Rahmen der Registrierung MUSS die Organisation durch Vorlage eines Sicherheitsgutachtens nachweisen, dass sie die durch die gematik vorgegebenen Mindestanforderungen erfüllt. Die Vorgaben für die Mindestanforderungen und das Vorgehen bei der Registrierung werden in [gemPKI_Reg] beschrieben.

Für eine Registrierung als CVC-CA kommen nur solche Organisationen in Frage ([gemSiKo#B4.5.3]),

- deren Hauptsitz in einem Land der Europäischen Union liegt und
- deren Betriebsstätte für den tatsächlichen Betrieb der CVC-CA in einem Land der Europäischen Union liegt.

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. Folgende Tabelle zeigt die aktuellen Vorgaben:

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.

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

Zwischen den verschiedenen CVC-PKIen für die verschiedenen Generationen wird es keine Cross-Zertifizierung geben. Falls zukünftig benötigt, MUSS eine Interoperabilität bei der C2C-Authentisierung zwischen Chipkarten verschiedener Generationen durch Maßnahmen außerhalb der CVC-PKIen sichergestellt werden.

4.2.4 Schlüsselversionen bei Root-CA und CAs

Root-CA und CAs der zweiten Ebene setzen für das Ausstellen von CV-Zertifikaten ein Schlüsselpaar ein, dass eine gegebene feste Schlüssellänge hat. Ebenso wird das Schlüsselpaar nur mit einem bestimmten kryptographischen Algorithmus genutzt. Aufgrund fortschreitender Erkenntnisse bezüglich der Sicherheit bestimmter Schlüssellängen bzw. Algorithmen wird nach gewissen zeitlichen Abständen die Nutzung eines neuen (längeren) Schlüsselpaares und ggf. auch die Nutzung neuer kryptographischer Algorithmen für die Root-CA bzw. eine der CAs der zweiten Ebene notwendig. Ein Wechsel zu einem neuen Schlüsselpaar mit einer größeren Schlüssellänge (und ggf. zu einem neuen Algorithmus) wird als Generationswechsel der Root-CA bzw. CA bezeichnet. Dieser Generationswechsel bei einer CA MUSS mit dem Generationswechsel bei den Chipkarten der Telematikinfrastruktur koordiniert werden. Siehe Abschnitt 4.2.3 zu der Interoperabilität bei verschiedenen Generationen.

Es kann weitere Gründe für den Wechsel des Schlüsselpaares geben wie z. B. organisatorische Vorgaben (z. B. Wechsel des Schlüsselpaares alle x Jahre) bzw. die Kompromittierung des aktuellen Schlüsselpaares. In diesen Fällen hat das neue Schlüsselpaar die gleiche Länge wie das alte Schlüsselpaar. Ein solcher Wechsel des Schlüsselpaares durch eine CA wird als Versionswechsel bezeichnet. Bei einem Versionswechsel werden die genutzten kryptographischen Algorithmen nicht geändert.

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.

Kommt es bei einer CA der zweiten Ebene zu einem Versionswechsel bei dem Schlüsselpaar für das Ausstellen von CV-Zertifikaten, kann dieser Fall logisch behandelt werden wie das Aufsetzen einer neuen CA. Die CA MUSS den öffentlichen Schlüssel ihres neuen Schlüsselpaares durch die Root-CA zertifizieren lassen. Bei allen im Folgenden durch die CA zu erzeugenden CV-Zertifikate MUSS das neue Schlüsselpaar verwendet werden. Entsprechend MUSS bei der Kartenproduktion das durch die Root-CA ausgestellte neue CV-Zertifikat der CA in die zugehörigen Karten eingebracht werden.

Ein Versionswechsel bei dem Schlüsselpaar bei der Root-CA wird auch als Wechsel der Root-Version bezeichnet. Alle CV-Zertifikate, die direkt (CV-Zertifikate für eine CA) bzw.

indirekt (CV-Zertifikate für eine eGK/HBA/SMC) von einem bestimmt Schlüsselpaar der Root-CA abhängen, gehören zur gleichen Root-Version.

Kommt es bei der Root-CA zu einem Wechsel der Root-Version, so hat dies (aus logischer Sicht) die gleiche Wirkung wie der Aufbau einer zweiten neuen PKI für die CV-Zertifikate. Eine übergeordnete Root für alle Chipkarten existiert dann nicht mehr. Zum Beispiel kann dann eine eGK, deren CV-Zertifikat zu einer Root-Version gehört, nicht mehr ohne weiteres eine C2C-Authentisierung mit einem HBA durchführen, dessen CV-Zertifikat zu einer anderen Root-Version gehört.

Damit auch nach einem Wechsel der Root-Version die C2C-Authentisierung zwischen zwei Chipkarten durchgeführt werden kann, wird das folgende Vorgehen umgesetzt:

- Führt die Root-CA einen Wechsel der Root-Version durch, MUSS sie zwei so genannte Cross-CV-Zertifikate erzeugen, und zwar eins über ihren neuen öffentlichen Schlüssel mit ihrem aktuellen privaten Schlüssel und eins über ihren aktuellen öffentlichen Schlüssel mit ihrem neuen privaten Schlüssel.

- Diese beiden Cross-CV-Zertifikate MÜSSEN auf einem Server der Root-CA Dritten zur Verfügung gestellt werden, d. h. Komponenten, die diese Cross-CV-Zertifikate benötigen, können diese über einen Download vom Server laden. Die Verantwortung, dass eine Komponente bezüglich der vorhandenen Cross-CV-Zertifikate den aktuellen Stand hat, liegt bei dem Betreiber der Komponente.

- Wird nun an einer Komponente (z. B. Konnektor) eine C2C-Authentisierung zwischen zwei Chipkarten durchgeführt, geschieht dies wie folgt: Zunächst werden aus beiden Chipkarten die CA-CV-Zertifikate ausgelesen. Anhand der in dem Zertifikatsfeld CAR enthaltenen Schlüssel-Referenzierung können die Root-Versionen ermittelt werden, zu der die CV-Zertifikate der beiden Karten gehören. Gehören die Karten zu unterschiedlichen Root-Versionen, MÜSSEN vor der eigentlichen C2C-Authentisierung die entsprechenden Cross-CV-Zertifikate der Root-CA in die Chipkarten geladen werden. Dabei kann es ggf. notwendig sein, mehrere Cross-CV-Zertifikate in korrekter Reihenfolge in eine Chipkarte zu laden.

Die zu einer Root-Version gehörenden zwei Cross-CV-Zertifikate MÜSSEN in den betroffenen Komponenten solange gespeichert bleiben, wie noch Chipkarten (eGK/HBA/SMC) mit CV-Zertifikaten dieser Root-Version im Felde aktiv sind. Eine klare Abgrenzung dieses Zeitraumes ist zurzeit nicht möglich. Die Root-CA wird auf ihrem Server bekannt geben, falls zu Root-Version gehörende Cross-CV-Zertifikate gelöscht werden können.

Die tatsächliche Durchführung des Wechsels der Root-Version MUSS durch die beteiligten Organisationen des Gesundheitsinfrastuktur entschieden werden, wobei sowohl technische als auch betriebswirtschaftliche Faktoren berücksichtigt werden. Organisatorisch werden dabei die folgenden Eckpunkte eingehalten:

- Falls ein "normaler" Wechsel der Root-Version durchgeführt wird, MUSS dies zum 1. Januar eines Jahres geschehen. Nur notfallmäßige Wechsel der Root-Version werden im Laufe eines Jahres durchgeführt.

- Bei einem "normalen" Wechsel der Root-Version MUSS das neue Schlüsselpaar rechtzeitig vorher generiert werden, so dass die beiden

zugehörigen Cross-CV-Zertifikate spätestens im Oktober des vorherigen Jahres auf dem Server der Root-CA für einen Download zur Verfügung stehen. Entsprechend MUSS die Entscheidung über die Durchführung eines normalen Wechsels der Root-Version spätestens im August des vorherigen Jahres gefällt werden.

In CV-Zertifikaten, die durch die Root-CA für eine CA der zweiten Ebene ausgestellt werden, gilt das Folgende für die Schlüssel-Referenzierung des Root-Schüsselpaares (enthalten in dem Zertifikatsfeld CAR des CV-Zertifikats einer CA, siehe auch [gemPKI_Reg#A.2.2]):

- Über die Informationen der Felder Service-Indikator, CA-spezifische Information, Algorithmen-Referenz und Datum wird sichergestellt, dass eine eindeutige Zuordnung zu der korrekten Root-Version gegeben ist.
- Das in dem Feld CAR enthaltene Datum enthält insbesondere die beiden letzten Ziffern des Jahres, in dem die Root-CA den Wechsel der Root-Version durchgeführt hat.

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 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 bezüglich der durch die CV-Zertifikate geschützten Anwendungen unterbunden werden. Dies KANN z. B. durch Einzug der Chipkarte durch den Kartenherausgeber realisiert werden.
- 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 Fachliche Prozesse für die Root-CA

Im Folgenden werden die fachlichen Prozesse überblicksartig angegeben, die bei der Arbeit der Root-CA durchgeführt werden müssen. Die genauen Abläufe bei der

Durchführung eines der Prozesse sind im Rahmen der Feinspezifikation der Root-CA (durch den Betreiber der Root-CA) zu spezifizieren.

4.3.1 Generierung eines neuen Schlüsselpaares für die Root-CA

Dieser Prozess umfasst auch die Generierung des ersten Schlüsselpaares (erste Generation) im Rahmen des initialen Aufsetzens der Root-CA

Für die Arbeit der Root-CA wird ein neues Schlüsselpaar generiert. Dieses steht ab einem gegebenen Zeitpunkt für das Ausstellen neuer CV-Zertifikate zur Verfügung. Der zugehörige öffentliche Schlüssel MUSS geeignet veröffentlicht werden. Für das neue Schlüsselpaar MUSS das Backup geregelt werden.

Teilprozesse:

1a) Generierung des neuen Schlüsselpaares

MUSS intern in dem verwendeten HSM angestoßen werden.

1b) Backup für das neue Schlüsselpaar erzeugen

Abhängig von dem gewählten Vorgehen beim Backup der Root-CA (siehe Abschnitt „Grundlagen für die Sicherheit“) MUSS ein Backup für das neue Schlüsselpaar erstellt werden.

1c) Veröffentlichung des öffentlichen Schlüssels

Der öffentliche Schlüssel MUSS aus dem HSM ausgelesen werden. Dieser MUSS dann in geeigneter Form veröffentlicht werden. Insbesondere MÜSSEN alle Datenaufbereiter/ Kartenproduzenten den öffentlichen Schlüssel erhalten. Anforderungen an den Prozess siehe Abschnitt „Grundlagen für die Sicherheit“.

1d) Information der CAs der zweiten Ebene

Die CAs der zweiten Ebene MÜSSEN über den Vorgang informiert werden.

1e) Cross CV-Zertifikate erzeugen

Dieser Teilprozess wird bei der Generierung des ersten Schlüsselpaares nicht benötigt.

Mit dem aktuellen Schlüsselpaar MUSS ein Cross-CV-Zertifikat über den öffentlichen Schlüssel des neuen Schlüsselpaares und mit dem neuen Schlüsselpaar ein Cross-CV-Zertifikat über den öffentlichen Schlüssel des aktuellen Schlüsselpaares erzeugt werden.

1f) Cross CV-Zertifikate bereitstellen

Dieser Teilprozess wird bei der Generierung des ersten Schlüsselpaares nicht benötigt.

Damit eGK, HBA und SMC an einem Konnektor eine C2C-Authentisierung auch dann durchführen können, falls ihre jeweiligen CV-Zertifikate zu verschiedenen Root-Versionen gehören, MUSS der Konnektor über die entsprechenden Cross-CV-Zertifikate der Root-CA verfügen. Die Root-CA stellt daher die erzeugten Cross-CV-

Zertifikate auf einem Server für einen Download durch die betroffenen Komponenten zur Verfügung.

1g) Neues Schlüsselpaar aktivieren

Das neue Schlüsselpaar MUSS indem HSM aktiviert werden. Von diesem Zeitpunkt an werden alle CA-CV-Zertifikate mit dem neuen Schlüsselpaar erzeugt.

Generierung und Aktivierung des neuen Schlüsselpaares fallen im Allgemeinen zeitlich auseinander, damit die zugehörigen Cross-CV-Zertifikate rechtzeitig vor der eigentlichen Aktivierung zu einem Download zur Verfügung gestellt werden können.

Die beiden letzten Ziffern des Jahres, die die Root-CA als Datum in ein CV-Zertifikat ein CA in das Feld CAR einträgt, beziehen sich auf das Jahr der Aktivierung des Schlüssels und nicht auf das Jahr seiner Generierung.

4.3.2 Registrierung der CAs der zweiten Ebene

Dieser Prozess wird nicht durch den technischen Betreiber der Root-CA durchgeführt, sondern durch die gematik. Bei der gematik liegt dabei die Verantwortung für die Entscheidung, ob eine CA erfolgreich registriert werden kann oder nicht. Mit Teilaufgaben dieses Prozesses kann die gematik externe Dienstleister beauftragen.

Eine CA MUSS sich bei der Root-CA registrieren lassen bevor sie ein entsprechendes CV-Zertifikat über ihren öffentlichen Schlüssel beantragen kann.

Die Registrierung einer CA wird detailliert in [gemPKI_Reg] beschrieben.

Teilprozesse (aus Sicht der Root-CA):

2a) Antrag entgegennehmen

2b) Antrag überprüfen

2c) Ergebnis der antragstellenden CA mitteilen

2d) Ergebnis in interne CA-Datenbank übernehmen

In der CA-Datenbank werden alle relevanten Informationen der erfolgreich registrierten CAs der zweiten Ebene vorgehalten. Die Informationen dieser Datenbank werden u. a. bei folgenden Prozessen benötigt:

- Information der CAs der zweiten Ebene über die Generierung eines neuen Schlüsselpaares für die Root-CA.
- Überprüfung des Antrages eines CA auf Ausstellung eines neuen CV-Zertifikates.

2e) Nachweis in interne Registrierung-Protokollierung übernehmen

Antrag, Ergebnis und Begründung müssen in die interne Registrierung-Protokollierung übernommen werden. Die Inhalte der Protokollierung MÜSSEN einen revisionssicheren Nachweis über das ordnungsgemäße Arbeiten der Root-CA ermöglichen.

4.3.3 Ausstellen eines neuen CV-Zertifikats für eine CA der zweiten Ebene

Auf Antrag wird für eine CA der zweiten Ebene ein neues CV-Zertifikat über ihren öffentlichen Schlüssel mit dem aktuellen Schlüsselpaar der Root-CA erzeugt. Das neue CV-Zertifikat wird danach an die CA übermittelt. Ein Nachweis über diesen Vorgang wird in die interne Zertifikatsprotokollierung der Root-CA übernommen.

Teilprozesse (aus Sicht der Root-CA):

3a) Antrag entgegennehmen

Der Antrag auf Ausstellung eines neuen CV-Zertifikates muss von der CA übermittelt werden und durch die Root-CA entsprechend entgegengenommen werden.

3b) Antrag und öffentlichen Schlüssel überprüfen

Der Antrag MUSS überprüft werden. Dazu gehört:

- Der Antrag MUSS vom Aufbau her korrekt sein.
- Der Antrag MUSS von einer CA stammen, die sich vorher bei der Root-CA hat registrieren lassen.
- Die Authentizität des im Antrag enthaltenen öffentlichen Schlüssels sowie der Nachweis über den Besitz (vom Antragsteller) des zugehörigen privaten Schlüssels MUSS überprüft werden.

Ggf. wird der Antrag abgelehnt und mit einer entsprechenden Begründung an den Absender zurückgesendet.

3c) CV-Zertifikat erzeugen

Mit dem aktuellen Schlüsselpaar der Root-CA wird ein CV-Zertifikat über den im Antrag enthaltenen öffentlichen Schlüssel erstellt.

3d) CV-Zertifikat an CA übermitteln

Das neu erstellt CV-Zertifikat MUSS an die CA übermittelt werden, die den Antrag gestellt hat.

3e) Nachweis in interne Zertifikatsprotokollierung übernehmen

Antrag und neu erstelltes CV-Zertifikat MÜSSEN in die interne Zertifikatsprotokollierung übernommen werden.

Anmerkung: Diese interne Zertifikatsprotokollierung dient nicht dazu, die ausgestellten CV-Zertifikate für Dritte abrufbereit vorzuhalten, d. h. sie ist kein Verzeichnisdienst. Die Inhalte der Protokollierung sollen vielmehr einen revisionssicheren Nachweis über das ordnungsgemäße Arbeiten der Root-CA ermöglichen.

Weitere Details über Beantragung und Ausstellung eines CV-Zertifikats für eine CA werden in [gemPKI_Reg] beschrieben.

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 benötigten Daten) die Herstellung

- echter eGKs für Versicherte,
- echter HBAs/SMCs mit Profilen für beliebige Rollen (Arzt, Apotheker, etc.)
- echter SMCs mit Profilen für beliebige Geräte (SMC-K, SMC-RFID, etc.).

Ein einmal ausgestelltes CV-Zertifikat hat eine unbegrenzte Gültigkeit[1]. Vor diesem Hintergrund muss durch die Sicherheitspolitik der PKI für CV-Zertifikate verhindert werden, dass CV-Zertifikate unautorisiert erzeugt bzw. für einen nicht autorisierten Zweck erstellt werden.

In diesem Abschnitt werden Grundlagen für die Sicherheit „aus qualitativer Sicht“ angegeben. Dabei werden

- technische Vorgaben für die Sicherheit,
- organisatorische Vorgaben für die Sicherheit und
- betriebliche Vorgaben für die Sicherheit

unterschieden. Die Vorgaben für die Sicherheit MÜSSEN dann in den Feinspezifikationen und Betriebskonzepten für die Root-CA und den CAs der zweiten Ebene umgesetzt werden. Über die Umsetzung MUSS ein Sicherheitskonzept erstellt werden.

Die im Folgenden angegebenen Vorgaben müssen als Mindestanforderungen verstanden werden. Aufgrund der zentralen Bedeutung der PKI für CV-Zertifikate für die Sicherheit der Telematikinfrastruktur MUSS sowohl bei der Root-CA als auch bei den CAs der zweiten Ebene ein vergleichbares Sicherheitsniveau umgesetzt werden, wie es zum Beispiel bei ZDAs für eine Ausgabe von qualifizierten Zertifikaten in den (auch für die PKI der CV-Zertifikate) relevanten Bereichen umgesetzt werden muss.

Die Abgrenzung der nachfolgenden Festlegungen zum übergreifenden Sicherheitskonzept der Telematikinfrastruktur [gemSiKo] gemäß Abschnitt 2.5 ist zu beachten.

Die Betreiber der einzelnen CAs können ihre Sicherheitskonzepte und deren Umsetzung frei nach eigenen Vorgaben bzw. den Vorgaben ihrer Auftraggeber (z. B. Kartenherausgeber) gestalten, sofern die im Folgenden enthaltenen Vorgaben mindestens erfüllt sind. Eine CA der zweiten Ebene muss sich bei der gematik registrieren lassen. Im Rahmen dieser Registrierung muss die Einhaltung der Vorgaben durch ein Sicherheitsgutachten nachgewiesen werden.

[1] Die Gültigkeit eines einzelnen CV-Zertifikats einer eGK/HBA/SMC wird durch die Nutzbarkeit der Chipkarte eingeschränkt. CV-Zertifikate verlieren aber auch ihre Gültigkeit (bzw. können nicht mehr erfolgreich bei einer C2C-Authentisierung eingesetzt werden), falls die zur entsprechenden Root-Version gehörenden Cross-CV-Zertifikate der Root-CA aus den Konnektoren gelöscht werden (siehe Abschnitt 4.2.4).

4.4.1 Sicherheitsanforderungen und Schutzbedarf

Durch die Kompromittierung der Sicherheit der Root-CA oder auch nur der Sicherheit einer der CAs der zweiten Ebene wird die gesamte PKI für die CV-Zertifikate kompromittiert. Für die Arbeit der Root-CA und der CAs der zweiten Ebene müssen daher Sicherheitskonzepte durch die einzelnen CAs erstellt werden. Die gematik gibt dabei Mindeststandards für die Sicherheitsanforderungen an die einzelnen CAs der zweiten Ebene vor.

Bei der Erstellung der Sicherheitskonzepte müssen u. a. die in der folgenden Tabelle enthaltenen Angaben zu Schutzbedarf und Sicherheitszielen berücksichtigt werden:

Tabelle 3 – Schutzbedarf

Sicherheitsziel	Schutzbedarf	Erläuterung	Aufwand
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 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 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.

Sicherheitsziel	Schutzbedarf	Erläuterung	Aufwand
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 muss registrieren, welcher Karteninhaber welche Karte (HBA/SMC) erhalten hat.	Hoch: Protokollierung aller ausgestellter CV-Zertifikate.mit einem Zugriffsprofil ungleich 0.
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. 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.

Eine CA MUSS grundsätzlich alle solche CV-Zertifikate revisionssicher protokollieren, 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]).

Anmerkung: Die Nachvollziehbarkeit der Ausgabe von CV-Zertifikaten mit einem Zugriffsprofil ungleich 0 (in einem HBA bzw. einer SMC) kann nur durch die Zusammenarbeit von dem für die Chipkarte verantwortlichen Kartenherausgeber und der das CV-Zertifikat erzeugenden CA umgesetzt werden. Die CA muss dazu die CV-Zertifikate, die Zuordnung zu den Chipkarten (Certificate Holder Reference) sowie den verantwortlichen Kartenherausgeber protokollieren [gemPKI_Reg]. Die Protokollierung der Zuordnung einer Chipkarte zu dem Karteninhaber (Heilberufler bzw. Organisation des Gesundheitswesens) liegt jedoch in der Verantwortung des Kartenherausgebers.

4.4.2 Sicherheit bei der Root-CA

Für die Sicherheit der Root-CA gelten die gleichen in [gemPKI_Reg#6] beschriebenen Mindestanforderungen wie bei einer CA der zweiten Ebene mit den folgenden Abweichungen bzw. Ergänzungen:

Technische Vorgaben:

- Für das HSM der Root-CA DARF mit Ausnahme eines zweiten HSMs für Backup-Zwecke ein weiterer Klon NICHT erzeugt werden.
- Für das HSM der Root-CA MUSS ein Backup-HSM erzeugt werden. Die dabei möglichen Alternativen werden unten beschrieben.
- Der öffentliche Schlüssel der Root-CA MUSS auf den Internetseiten des Betreibers für einen Download zur Verfügung gestellt werden. Dabei MUSS die Integrität und Authentizität des öffentlichen Schlüssels sichergestellt sein (gemSiKo#B4.5.1)
- Der Betreiber der Root-CA MUSS einen Fingerprint über seinen öffentlichen Schlüssel auf Anfrage per Briefpost zur Verfügung stellen.
- Wird ein Wechsel der Root-Version durchgeführt, MUSS der Betreiber die zugehörigen Cross-CV-Zertifikate erzeugen und auf seinen Internetseiten für einen Download zur Verfügung stellen. Dabei MUSS die Integrität und Authentizität der Cross-CV-Zertifikate sichergestellt sein (gemSiKo#B4.5.3)
- Der Betreiber der Root-CA MUSS die Verfügbarkeit seiner Internetseiten für einen Download seiner öffentlichen Schlüssel und Cross-CV-Zertifikate sicherstellen.

Für die Realisierung des benötigten Backup-HSMs 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 aus [gemSiKo#B4.5.4] 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 eine Registrierung einer CA der zweiten Ebene 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.

4.4.3 Sicherheit bei einer CA der zweiten Ebene

Eine CA der zweiten Ebene wird im Auftrage eines Kartenherausgebers einer eGK, eines HBA oder einer SMC betrieben. Der Betreiber einer CA der zweiten Ebene kann in Abstimmung mit dem ihn beauftragenden Kartenherausgeber Konzeption, Realisierung und Betrieb seiner CA weitestgehend gemäß eigenen Vorgaben durchführen.

Probleme bei der Sicherheit einer CA der zweiten Ebene können die Sicherheit der gesamten PKI für CV-Zertifikate und somit des gesamten Systems der elektronischen Gesundheitskarte gefährden. Für die Sicherheit einer CA der zweiten Ebene werden daher durch die gematik Vorgaben erstellt, die als Mindeststandard bei der Sicherheit der CA umgesetzt werden MÜSSEN. Im Folgenden werden diese Vorgaben für den Mindeststandard beschrieben.

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.

Die Mindestanforderungen an die Sicherheit einer CA der zweiten Ebene werden in [gemPKI_Reg#6] beschrieben.

4.5 Ausstellen eines CV-Zertifikates für eine CA

Durch das Ausstellen eines CV-Zertifikates für eine CA erhält diese die Möglichkeit, eigene CV-Zertifikate mit ihrem Schlüsselpaar nicht nur zu erzeugen sondern Chipkarten auch mit diesen korrekt zu personalisieren. Erst durch Ausstellung des CV-Zertifikates wird eine CA in die Lage versetzt, (zusammen mit einem Kartenhersteller) eGKs, HBAs oder SMCs zu erstellen, die in dem Gesamtsystem im Rahmen einer C2C-Authentisierung als „Echt“ erkannt werden. Der Prozess des Ausstellens eines CV-Zertifikates für eine CA ist daher für die Sicherheit des Gesamtsystems von entscheidender Bedeutung. Es MUSS sichergestellt werden,

- dass nur für vorher registrierte CAs ein entsprechendes CV-Zertifikat ausgestellt wird,
- dass der dabei zertifizierte öffentliche Schlüssel authentisch ist und
- dass die CA auch wirklich den zugehörigen privaten Schlüssel besitzt.

Im Folgenden wird ein Überblick über den Prozess für das Ausstellen eines CV-Zertifikates für eine CA gegeben. Details werden in [gemPKI_Reg] beschrieben. Es wird

davon ausgegangen, dass der Prozess aus Sicht einer CA nur selten auszuführen ist und dass der Prozess aus Sicht der Root-CA nur für wenige CAs der zweiten Ebene ausgeführt wird. Die einzelnen Schritte sind:

(1) Die CA erzeugt mit seinem HSM einen signierten PKCS#10-Request für seinen öffentlichen Schlüssel. Dieser wird ausgegeben und auf einem geeigneten Medium (z. B. USB-Stick) gespeichert.

(2) Über den öffentlichen Schlüssel wird ein Fingerprint gerechnet und auf einem Begleitschreiben ausgedruckt. Das Begleitschreiben wird per Post an die Root-CA gesendet.

(3) Ein Mitarbeiter der CA geht mit dem Medium zu der Root-CA. Dieser Mitarbeiter muss für die Ausübung dieser Rolle (Antragsteller CA-CV-Zertifikat oder Leiter/ Sicherheitsbeauftragter der CA) berechtigt sein. Dies wurde der Root-CA im Rahmen der Registrierung mitgeteilt.

(4) Die Root-CA überprüft die Personalien des Mitarbeiters der CA. Dadurch wird sichergestellt, dass die CA authentisch in dem Prozess vertreten wird.

(5) Die Root-CA überprüft, ob die CA aktuell gültig registriert ist.

(6) Von dem Medium werden der signierte PKCS#10-Request der CA ausgelesen. Die Signatur wird mit dem (in dem Request enthaltenen) öffentlichen Schlüssel überprüft. Dadurch wird sichergestellt, dass die CA tatsächlich über den zugehörigen privaten Schlüssel verfügt.

(7) Über den (in dem Request enthaltenen) öffentlichen Schlüssel wird ein Fingerprint gerechnet und mit dem Fingerprint verglichen, der vorher per Post in dem Begleitschreiben an die Root-CA gesendet wurde. Dadurch wird sichergestellt, dass der öffentliche Schlüssel authentisch ist.

(8) Das CV-Zertifikat über den öffentlichen Schlüssel wird durch das HSM der Root-CA gerechnet und ausgegeben. Das CV-Zertifikat wird auf ein Medium (z. B. USB-Stick) geschrieben und dem Mitarbeiter der CA übergeben.

(9) Nach Rückkehr wird das CV-Zertifikat von dem Medium ausgelesen und in die entsprechenden Systeme der CA eingebracht. Das eingebrachte CV-Zertifikat wird mit dem veröffentlichten öffentlichen Schlüssel der Root-CA verifiziert. Dadurch wird dessen Korrektheit sichergestellt.

4.6 Unterscheidung Testbetrieb – Produktivbetrieb

Für die PKI für CV-Zertifikate MUSS zwischen einem Produktivbetrieb und einem Testbetrieb unterschieden werden. Entsprechend wird bei den CV-Zertifikaten zwischen Poduktiv-CV-Zertifikaten und Test-CV-Zertifikaten unterschieden.

Sowohl Root-CA als auch die CAs der zweiten Ebene MÜSSEN das Ausstellen von Test-CV-Zertifikaten anbieten. Für das Ausstellen von Test-CV-Zertifikaten MÜSSEN spezielle Test-Schlüsselpaare in einer Test-CA eingesetzt werden. Test-CA und Produktiv-CA MÜSSEN technisch und organisatorisch geeignet getrennt werden.

Gemäß [gemSpec_MK#2.1] wird bei den Chipkarten neben den Produktivkarten noch zwischen Testlaborkarten, Musterkarten und Testkarten unterschieden. Testkarten

werden dabei im Rahmen von Feldtests eingesetzt und enthalten wie Produktivkarten bereits Echtdaten der Versicherten bzw. Leistungserbringer. Es gilt daher folgende Zuordnung aus [gemSpec_MK#2.1]:

- Produktivkarten und Testkarten enthalten Produktiv-CV-Zertifikate. Diese MÜSSEN durch eine Produktiv-CA erzeugt werden, deren CA-Zertifikat aus der Produktiv-Root-CA der gematik abgeleitet wurde.
- Musterkarten enthalten Test-CV-Zertifikate. Diese MÜSSEN durch eine Test-CA erzeugt werden, deren CA-Zertifikat aus der Test-Root-CA der gematik abgeleitet wurde.
- CV-Zertifikate für Testlaborkarten werden im Rahmen einer eigenständigen CVC-PKI erzeugt, deren Beschreibung nicht Bestandteil dieses Dokuments ist.

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 für das Austesten neuer Produkte Musterkarten benötigen.

Anhang

A1 – Abkürzungen

Kürzel	Erläuterung
C2C	card to card
CA	certification authority
CV	card verifiable
CVC	card verifiable certificate
eGK	Elektronische Gesundheitskarte
HBA	Heilberufeausweis
HPC	Oberbegriff für HBA und SMC
HSM	Hochsicherheitsmodul
PKI	Public Key Infrastructure
Root	Oberste CA in einer Hierarchie einer PKI
SigG	Signaturgesetz
SMC	security module card
ZDA	Zertifizierungsdienstleistungsanbieter (in diesem Dokument nur genutzt, falls qualifizierte (X.509-) Zertifikate ausgegeben werden)

A2 – Glossar

Das Glossar wird als zentrales Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Referenzierete Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[14890–1]	EUROPEAN STANDARD, DRAFT, prEN 14890-1, February 2007 Application Interface for smart cards used as secure signature creation devices – Part 1: Basic services
[14890–2]	EUROPEAN STANDARD, DRAFT, prEN 14890-2, February 2007 Application Interface for smart cards used as secure signature creation devices – Part 2: Additional services
[gemBetr_BK]	gematik (Draft 2008): Einführung der Gesundheitskarte – Betriebskonzept (nicht öffentlich)
[gemGesArch]	gematik (18.03.2008): Einführung der Gesundheitskarte – Gesamtarchitektur, Version 1.3.0
[gemPKI_Reg]	gematik (18.03.2008): Einführung der Gesundheitskarte - PKI für CV-Zertifikate, Registrierung einer CVC-CA der zweiten Ebene Version 1.5.0
[gemSiKo]	gematik (10.03.2008): Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur Version 2.2.0
[gemSpec_eGK _P1]	gematik (20.03.2008): Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte; Teil 1 – Spezifikation der elektrischen Schnittstelle Version 2.2.0
[gemSpec _eGK _P2]	gematik (25.03.2008): Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte ; Teil 2 – Grundlegende Applikationen Version 2.2.0
[gemSpec_Krypt]	gematik (26.03.2008): Einführung der Gesundheitskarte – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 1.3.0
[gemSpec_MK]	gematik (22.02.2008): Einführung der eGK - Spezifikation für Musterkarten und Testkarten (eGK, HBA, SMC) Version 2.6.0
[HPC-P1]	BundesÄrzteKammer et.al. (in Vorbereitung): German Health Professional Card and Security Module Card, Part 1: Commands, Algorithms and Functions of the COS Platform Version 2.x.x
[HPC-P2]	BundesÄrzteKammer et.al. (in Vorbereitung): German Health Professional Card and Security Module Card, Part 2: HPC Application and Functions Version 2.x.x
[HPC-P3]	BundesÄrzteKammer et.al. (in Vorbereitung): German Health Professional Card and Security Module Card, Part 2: SMC Application and Functions

	Version 2.x.x
[ISO7816-8]	ISO (2004): Identification cards – Integrated circuit cards – Part 8: Commands for security operations

A6 - Klärungsbedarf

Kap.	Offener Punkt	Zuständig
4.2.5	Es muss noch geklärt werden, ob ggf. doch ein Sperren einzelner CV-Zertifikate in der PKI umgesetzt werden soll, und falls ja, wie diese Funktion umzusetzen ist.	ITS/AP, ITS/SI, SPE/ZD