gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

PKI für CV-Zertifikate

Registrierung einer CVC-CA der zweiten Ebene

Version:	1.5.0
Stand:	18.03.2008
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

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

- Kapitel 3 wurde zur Darstellung der Eingangsanforderungen eingefügt. Die Anforderungen müssen noch mit dem Anforderungsmanagement abgestimmt werden.
- Die neuen Gegebenheiten bei den Karten der Generation 1 wurden berücksichtigt.
- Ein kurzer Abschnitt zu dem Thema "Interoperabilität zwischen verschiedenen Kartengenerationen" wurde eingefügt.
- Bei den Sicherheitsanforderungen wurden auf an den relevanten Stellen auf entsprechende Vorgaben aus dem gematik-Sicherheitskonzept verwiesen.
- Die Unterscheidung zwischen CV-Rollen-Zertifikaten und CV-Geräte-Zertifikate sowie die Unterscheidung zwischen Rollenauthentisierung und Geräteauthentisierung wurden eingeführt.
- Bei den SMCs wird nun an relevanten Stellen zwischen SMC-A und SMC-B sowie den neuen SMC-K und SMC-RFID unterschieden.
- In dem neuen Anhang wird der Aufbau der CV-Zertifikate beschrieben.
- Die Darstellung der Formulare für die Registrierung wurde aus dem Dokument entfernt und durch eine Referenz auf die Verfügbarkeit im Internet ersetzt.
- Die informativen Beispiele (in der alten Version Kapitel 8) wurden entfernt. Es ist zukünftig Aufgabe des Dienstleisters (Root-CVC-CA), entsprechende Beispiele vorzugeben.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemPKI_Reg]	gematik (18.03.2008): Einführung der Gesundheitskarte - Registrierung einer CVC-CA der zweiten Ebene Version 1.5.0

Dokumentenhistorie

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	13.04.06	alle	Dokument neu erstellt	gematik
0.0.2	26.04.06	alle	QS und Abstimmung mit BÄK	gematik
1.0.0	05.04.06		Abnahme QS und Freigabe	gematik
1.0.1	08.06.06	4 5.6 5.6.7 6.1	ergänzt um Abschnitt 4.1.6 Kosten ergänzt/geändert: "geklonte HSM" zugelassen Klarstellung eingefügt. um Hinweis auf CA-Name für Test-CVC-CA ergänzt.	gematik
1.1.0	14.06.06		Abnahme QS	gematik lQS
1.2.0	16.08.06	4.1.6, 5.5	Kostenverteilung aufgehoben Anforderungen an die Sicherheit des privaten Schlüssels ergänzt.	gematik
1.2.1	27.09.06	4.2 5.6.5, 6, 6.3	Präzisierung der Beschreibung des Registrierungsverfahrens und des erford. Sicherheitsgutachtens Hinweis auf Standardkonformität des PKCS#10 Requests	gematik
1.2.2	26.10.06	4.2, 7	Hinweis bei den Registrierungsanträgen auf elektronische Formulare und deren Handhabung	gematik
1.3.0	30.10.06		freigegeben	
1.3.1	20.11.06	4, 6.3	Editorische Überarbeitung	gematik
1.4.0	29.11.06		Freigabe	gematik
1.4.1	20.02.08		überarbeitet für Karten der Generation 1	SPE/ZD
1.4.2	13.03.08		Einarbeitung Kommentare gematik-interne QS	SPE/ZD
1.5.0	18.03.08		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Für eGKs, HBAs und SMCs verschiedener Ausprägungen ist in der Telematikinfrastruktur eine direkte Card-to-Card (kurz C2C) Authentisierung vorgesehen. Diese C2C-Authentisierung basiert auf in den Chipkarten gespeicherten privaten Schlüsseln und so genannten "card verifiable certificates" (CV-Zertifikate).

Für die CV-Zertifkate wird eine eigene CVC-PKI aufgebaut. CV-Zertifikate für eine eGK, einen HBA oder eine SMC werden im Rahmen der PKI für CV-Zertifikate durch eine CVC-CA der zweiten Ebene erzeugt. Die CV-Zertifikate (sowie die zugehörigen privaten Schlüssel) werden dann während der Kartenherstellung in die Chipkarten eingebracht.

Eine CVC-CA benötigt ein CA-CV-Zertifikat, welches von der Root-CVC-CA signiert wurde. Um dieses beantragen zu können, muss sich eine CVC-CA vorher bei der gematik registrieren lassen. Im Rahmen ihrer Verantwortung für die gesamte PKI für CV-Zertifikate gibt die gematik die Mindestanforderungen vor, die an die Sicherheit einer CVC-CA gestellt werden. Als Voraussetzung für die Registrierung muss die CVC-CA nachweisen, dass sie diese Mindestanforderungen erfüllt.

Die CVC-CA arbeitet bei der Kartenherstellung und Kartenauslieferung eng mit dem Kartenherausgeber und dem Kartenhersteller zusammen. Für die Sicherheit der PKI der CV-Zertifikate ist die Sicherheit des Gesamtprozesses für die Kartenherstellung bis zur Auslieferung an den Karteninhaber von Bedeutung. Entsprechende Anforderungen werden daher in diesem Dokument aufgestellt. Die Zusammenarbeit der Beteiligten kann sehr unterschiedlich organisiert werden. Aus Sicht der PKI für CV-Zertifikate ist die CVC-CA stellvertretend für alle Beteiligten für die Einhaltung der in diesem Dokument enthaltenen Anforderungen verantwortlich.

Das vorliegende Dokument beschreibt den Prozess der Registrierung einer CVC-CA durch die gematik. Dabei werden die Mindestanforderungen an eine CVC-CA aus [gemPKI_CVCGK] konkretisiert. Zusätzlich wird der Prozess für das Beantragen und Ausstellen eines CV-Zertifikates für eine CVC-CA durch die Root-CVC-CA detailliert beschrieben.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Chipkarten der Gesundheitstelematikinfrastruktur benötigen CV-Zertifikate. Die werden im Rahmen einer PKI für CV-Zertifikate erzeugt, die aus einer übergeordneten Root-CVC-CA und mehreren CVC-CAs der zweiten Ebene besteht.

CVC-CAs der zweiten Ebene müssen sich bei der gematik registrieren lassen. Dabei müssen sie u. a. nachweisen, dass die durch die gematik vorgegebenen Mindestanforderungen an die Sicherheit der CVC-CA erfüllt werden. Dieses Dokument beschreibt die Mindestanforderungen und den Prozess der Registrierung.

Zusätzlich wird beschrieben, wie eine vorher registrierte CVC-CA ihr benötigtes CA-CV-Zertifikat von der Root-CVC-CA erhält.

2.2 Zielgruppe

Dieses Dokument richtet sich an Betreiber einer CA, die CV-Zertifikate für eGKs, HBAs oder SMCs generieren.

2.3 Geltungsbereich

Die in diesem Dokument enthaltenen Vorgaben sind für alle Betreiber einer CA verbindlich, sofern sie mit dieser CA CV-Zertifikate für eGKs, HBAs oder SMCs generieren.

2.4 Arbeitsgrundlagen

Organisatorische Vorgaben wurden abgestimmt zwischen den Vertretern der Leistungserbringer und der Kostenträger.

Vorgaben bezüglich der Notwendigkeit und Durchführung der Registrierung einer CVC-CA ergeben sich aus dem Grobkonzept für die PKI für CV-Zertifikate [gemPKI_CVCGK].

Die Abstimmung technischer Abläufe und Vorgaben wurde mit dem Betreiber der Root-CVC-CA vorgenommen.

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-Authentikation 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. Das gleiche gilt für die Vorgaben bezüglich der Lebensdauer der Schlüssel (und damit implizit auch für die Gültigkeitsdauer der CV-Zertifikate).

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 1.4.0 vom 29.11.2006 dieses Dokuments.

Für die Anwendung QES einer eGK werden zur Absicherung des nachträglichen Download von qualifizierten Zertifikaten zum Teil auch CV-Zertifikate genutzt. Diese CV-Zertifikate werden nicht im Rahmen der diesem Dokument zu Grunde liegenden CVC-PKI erzeugt. Diese speziellen CV-Zertifikate werden daher in diesem Dokument nicht weiter betrachtet.

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 der sie nutzenden Komponenten/Prozesse 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	Anforderungs-nummer	Anforderungs-level	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_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 Freischaltung) und Geräteauthentisierung (ohne Freischaltung) erreicht

Quelle	Anforderungs-nummer	Anforderungs-level	Beschreibung
AM	A_02261 (alt: 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. …)
gemSiKo#B4.4.1	A_02695	MUSS	Die Karten (eGK, HBA, SMC) MÜSSEN CV-Zertifikate interpretieren und verarbeiten können.
gemSiKo#B4.4.1	A_02712	MUSS	Chipkarten, die vor Ausgabe an den Karteninhaber als fehlerhaft erkannt werden, MÜSSEN ordnungsgemäß vernichtet werden.
gemSiKo#B4.4.1	A_02713	MUSS	Chipkarten, die fehlerfrei produziert wurden, MÜSSEN an den vorgesehenen Karteninhaber übergeben werden.
gemSiKo#B4.5.3	A_02781	MUSS	Es MUSS für HBA und eGK eine PKI für CV-Zertifikate betrieben werden.
gemSiKo#B4.5.3	A_02782	MUSS	Der Entstehungs- und Sperrprozess eines konkreten CV-Zertifikats MUSS lückenlos einer verantwortlichen Stelle zuordenbar und nachvollziehbar sein.
gemSiKo#B4.5.3	A_02783	MUSS	Ein CV-Zertifikat DARF am zentralen Speicherort NICHT mehr verändert werden.
gemSiKo#B4.5.3	A_02784	MUSS	Der dezentrale Speicherort privater Schlüssel DARF nach der initialen Aufbringung der CV-Zertifikate NICHT mehr veränderbar sein.
gemSiKo#B4.5.3	A_02785	MUSS	Nicht mehr gültige private CVC-Schlüssel MÜSSEN dauerhaft und nachweislich vom weiteren Gebrauch ausgeschlossen werden.
gemSiKo#B4.5.3	A_02786	MUSS	Vor dem Generieren eines CV-Zertifikates MUSS sichergestellt sein, dass die Generierung auf Antrag eines hierfür Berechtigten erfolgt.
gemSiKo#B4.5.3	A_02787	MUSS	Vor der Produktion einer Chipkarte mit zugehörigem CV-Zertifikat MUSS sichergestellt sein, dass die Produktion nur im Auftrag eines berechtigten Kartenherausgebers erfolgt.
gemSiKo#B4.5.3	A_02788	MUSS	Es MUSS sichergestellt sein, dass in dem CV-Zertifikat einer Chipkarte nur ein für den Karteninhaber der Chipkarte zugelassenes Zugriffprofil kodiert ist.
gemSiKo#B4.5.3	A_02789	MUSS	In dem CV-Zertifikat einer Chipkarte MUSS die korrekte ICCSN der Chipkarte kodiert sein.
gemSiKo#B4.5.3	A_02790	MUSS	Nach Produktion MUSS in der Chipkarte der private Schlüssel enthalten sein, der zu dem durch das enthaltene CV-Zertifikat zertifizierten öffentlichen Schlüssel gehört.
gemSiKo#B4.5.3	A_02791	MUSS	In die Chipkarte MUSS der korrekte aktuelle öffentliche Schlüssel der relevanten Root-CVC-CA eingebracht werden.

Quelle	Anforderungs-nummer	Anforderungs-level	Beschreibung
gemSiKo#B4.5.3	A_02792	MUSS	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	A_02793	MUSS	Das (Sub-)CVC-CA Schlüsselpaar MUSS seine Gültigkeit verlieren, falls für seine Aufgaben ein neues Schlüsselpaar generiert wurde oder falls die Registrierung der CVC-CA durch die gematik widerrufen wurde. In diesem Fall MUSS das Schlüsselpaar vernichtet werden. Dies MUSS durch eine der folgenden Maßnahmen realisiert werden: o Physikalisches Zerstören des HSM (ggf. aller Klone), in dem der private Schlüssel gespeichert ist. Diese Maßnahme MUSS zwingend erfolgen, falls das HSM keine der beiden folgenden Möglichkeiten unterstützt. o Physikalisches Löschen des privaten Schlüssels innerhalb des HSM (ggf. innerhalb aller Klone), falls das HSM diese Funktionalität unterstützt. o Dauerhaftes Sperren aller möglichen Zugriffe auf den privaten Schlüssel innerhalb des HSM (ggf. innerhalb aller Klone), falls das HSM diese Funktionalität unterstützt.
gemSiKo#B4.5.3	A_02794	MUSS	Bei der Beantragung und Generierung des CA-CV-Zertifikates MUSS die Authentizität des öffentlichen Schlüssels sichergestellt werden.
gemSiKo#B4.5.3	A_02795	MUSS	Die Arbeit der CVC-CA MUSS revisionsfähig protokolliert werden. Folgende Ereignisse MÜSSEN dabei mindestens protokolliert werden: o Generierung eines neuen Schlüsselpaares im HSM, o Löschung eines privaten Schlüssels im HSM, o Export des privaten Schlüssels, o Import des privaten Schlüssels, o Sperrung der Zugriffe auf einen privaten Schlüssel im HSM, o Erzeugen eines CV-Zertifikats mit einem Profil ungleich 0, o Erzeugen einer Menge von CV-Zertifikaten mit Profil 0
gemSiKo#B4.5.3	A_02796	MUSS	Bei jedem Ereignis, welches durch eine CVC-CA revisionsfähig protokolliert werden muss, MÜSSEN die folgenden Werte protokolliert werden: o Datum und Uhrzeit, o Typ des Ereignisses, o Namen der beiden Mitarbeiter der CVC-CA, die das HSM freigeschaltet haben.
gemSiKo#B4.5.3	A_02797	MUSS	Beim Erzeugen eines CV-Zertifikates mit einem Profil ungleich 0 MÜSSEN zusätzlich die folgenden Werte protokolliert werden: o Name des zuständigen Kartenherausgebers, o Inhalt der Felder CHR und CHA, o das erstellte CV-Zertifikat selber

Quelle	Anforderungs-nummer	Anforderungs-level	Beschreibung
gemSiKo#B4.5.3	A_02798	MUSS	Beim Erzeugen eines CV-Zertifikates mit einem Profil gleich 0 MÜSSEN zusätzlich die folgenden Werte protokolliert werden: o Name des zuständigen Kartenherausgebers, o Anzahl der erzeugten CV-Zertifikate
gemSiKo#B4.5.3	A_02799	MUSS	Die Protokollierung bei dem Erzeugen von CV-Zertifikaten mit Profil gleich 0 SOLL pro Bestellung/Produktionslauf geschehen. Es MUSS dabei nachträglich anhand der Protokolle nachvollzogen werden können, wann wie viele CV-Zertifikate mit einem Profil gleich 0 für wen erzeugt wurden.
gemSiKo#B4.5.3	A_02800	MUSS	Alle Protokolldaten MÜSSEN bei ihrer Erstellung, Verarbeitung und Speicherung gegen mögliche Manipulationen geeignet geschützt werden.
gemSiKo#B4.5.3	A_02801	MUSS	Auf Antrag MUSS Vertretern der gematik Einblick in die Protokolle gewährt werden. Die Protokolldaten MÜSSEN dazu in einfacher verständlicher Form interpretierbar sein.
gemSiKo#B4.5.3	A_02802	MUSS	Die CVC-CA MUSS in ihrem Organisationskonzept (als Teil des Sicherheitskonzepts) mindestens die folgenden Rollen unterscheiden: o Leiter CVC-CA, o Sicherheitsbeauftragter CVC-CA, o Antragsteller CA-CV-Zertifikat, o Zertifizierer.
gemSiKo#B4.5.3	A_02803	MUSS	Das die CVC-CA realisierende Kernsystem (insbesondere das HSM) MUSS in einem geschützten Bereich der Betriebsstätte untergebracht sein. Für diesen Bereich MUSS gelten: o Falls zur CVC-CA gehörende Arbeitsplatz-Rechner oder Systeme außerhalb des geschützten Bereichs Zugriffe auf das Kernsystem in dem geschützten Bereich haben, MÜSSEN alle Zugriffe über diese Arbeitsplatz-Rechner bzw. Systeme auf das Kernsystem sowie die Kommunikation zwischen den Arbeitsplatz-Rechnern, den Systemen und dem Kernsystem gegen Manipulationen und unautorisierte Nutzung geeignet geschützt werden. o Ist die CVC-CA in ein Netzwerk eingebunden, MUSS sichergestellt werden, dass über das Netzwerk nicht auf die CVC-CA zugegriffen werden kann und dass keine Informationen der CVC-CA über das Netzwerk weitergegeben werden können.
gemSiKo#B4.5.3	A_02804	MUSS	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	A_02805	MUSS	Es wird im Regelbetrieb eine PKI mit einer CA-Hierarchie realisiert, d.h. es gibt untergeordnete CAs (im Folgenden immer nur CA genannt), die die Karten

Quelle	Anforderungs-nummer	Anforderungs-level	Beschreibung
			für den Wirkbetrieb ausgeben (eGK, HBA, SMC). Es MUSS sichergestellt sein, dass nur die Karten für den Wirkbetrieb mit medizinischen Echt-Daten in Kontakt kommen.
gemSiKo#B4.5.3	A_02806	MUSS	Es SOLL eine flache CA-Hierarchie eingesetzt werden.
gemSiKo#B4.5.3	A_02807	MUSS	Alle CAs MÜSSEN von der Telematikinfrastruktur genehmigt werden.
gemSiKo#B4.5.4	A_02808	MUSS	Falls notwendig KANN aus Gründen der Hochverfügbarkeit bzw. hoher Performanzanforderungen (Möglichkeit zur Lastverteilung) ein HSM "geklont" werden, indem der private Schlüssel aus dem HSM (kryptographisch abgesichert) exportiert und in ein weiteres HSM importiert wird. Dabei MÜSSEN die folgenden Punkte berücksichtigt werden: o Falls das Klonen eines HSM technisch möglich ist, MUSS der Vorgang in dem Sicherheitskonzept gesondert beschrieben und in dem Sicherheitsgutachten gesondert bewertet werden. Dabei MÜSSEN insbesondere die Maßnahmen für die Gewährleistung der Sicherheit des privaten Schlüssels als auch die (technischen und/oder organisatorischen) Maßnahmen für die Verhinderung des unautorisierten Erstellens von Klonen beschrieben (Sicherheitskonzept) und bewertet (Sicherheitsgutachten) werden. o Es MUSS sichergestellt sein, dass das Klonen eines HSM nur durch zwei Mitarbeiter (Vier-Augen-Prinzip) möglich ist. o Das Klonen eines HSM MUSS protokolliert werden. o Zu jeder Zeit MUSS einfach nachvollziehbar sein, wie viele Klone des HSM existieren. o Alle Klone eines HSM (d. h. alle HSM mit dem gleichen privaten Schlüssel) werden im Sinne dieses Dokuments logisch als ein HSM betrachtet, d.h. alle Anforderungen an ein HSM gelten für jeden Klon. o Alle Klone eines HSM (d. h. alle HSM mit dem gleichen privaten Schlüssel) MÜSSEN in einem geschützten Bereich der Betriebsstätte eingesetzt werden.

Quelle	Anforderungs-nummer	Anforderungs-level	Beschreibung
gemSiKo#B4.5.4	A_02809	MUSS	Es MUSS sichergestellt sein, dass folgende Funktionen des HSM nur nach einer Benutzerauthentikation zweier hierfür autorisierter Nutzer (Vier-Augen-Prinzip) möglich ist: o Generieren eines neuen Schlüsselpaares, o Berechnung einer Signatur mit dem privaten Schlüssel, o (kryptographisch abgesicherter) Export des privaten Schlüssels, o (kryptographisch abgesicherter) Import eines privaten Schlüssels, o Löschen des privaten Schlüssels (falls dies durch das HSM unterstützt wird), o Sperren der Zugriffe auf den privaten Schlüssel (falls dies durch das HSM unterstützt wird)

4 Grundlagen

4.1 Hierarchie der PKI für CV-Zertifikate

Für die CV-Zertifikate, die im Rahmen der Telematikinfrastruktur zum Einsatz kommen, existiert eine zweistufige PKI. Die kartenspezifischen CV-Zertifikate, die in eine eGK, einen HBA oder eine SMC eingebracht werden, werden dabei durch eine CA der zweiten Ebene (kurz CVC-CA) erzeugt. Die CV-Zertifikate der einzelnen CAs der zweiten Ebene werden durch die übergeordnete Root-CVC-CA erzeugt und an die CAs verteilt. Die folgende Abbildung zeigt die Zusammenhänge:

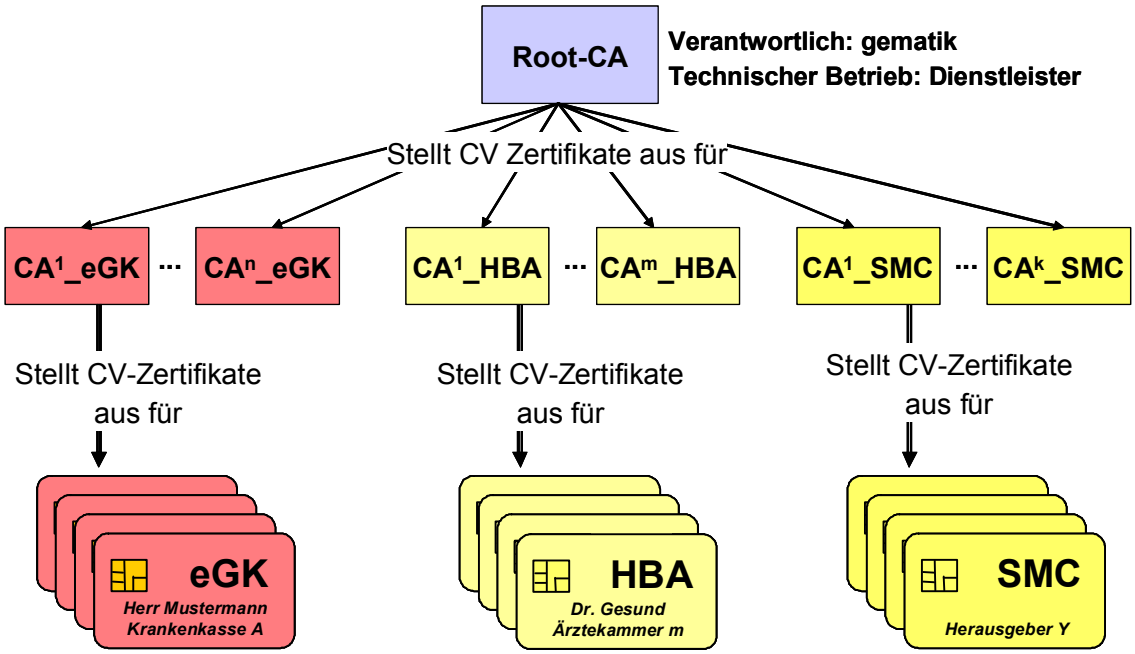

Abbildung 1 – Hierarchie der PKI für CV-Zertifikate

Die gesamte PKI MUSS dabei zweistufig sein, d.h. eine CA der zweiten Ebene darf ihrerseits nicht wieder CV-Zertifikate für Sub-CAs ausstellen. Dies bedeutet, dass ein CV-Zertifikat einer Chipkarte beim Verifizieren immer in zwei Schritten auf die Root zurückgeführt werden kann.

Die gematik ist im Auftrage der Organisationen der Telematikinfrastruktur verantwortlich für den Betrieb der Root-CVC-CA. Sie trägt damit insbesondere die Verantwortung für die Sicherheit und Funktionsfähigkeit der gesamten PKI für die CV-Zertifikate.

Die Funktion einer CVC-CA kann von Kartenherstellern, ZDAs oder den Kartenherausgebern selber übernommen werden. Diese CAs der zweiten Ebene arbeiten immer im Auftrage der für die Kartenherausgabe verantwortlichen Organisation.

Die gematik gibt (im Rahmen ihrer Verantwortung für die PKI der CV-Zertifikate) Mindestanforderungen an die Sicherheit, die Organisation und den Betrieb einer CVC-CA (durch dieses Dokument und durch [gemPKI_CVCGK]) vor. Voraussetzung für das

Ausstellen eines CV-Zertifikates für eine CVC-CA durch die Root-CVC-CA ist eine vorherige Registrierung der CVC-CA bei der gematik. Im Rahmen ihrer Registrierung muss die CVC-CA die Einhaltung der Mindestanforderungen nachweisen.

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. Folgende Tabelle zeigt die aktuellen Vorgaben:

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.

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.

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

Anmerkung: Die Vorgaben aus diesem Dokument in der vorliegenden Version gelten nur für die CVC-PKI für die Kartengeneration G1.

Anmerkung: Die konkreten Algorithmen, die für die Generation G2 basierend auf elliptischen Kurven verwendet werden sollen, werden noch festgelegt.

4.3 Aufbau eines CV-Zertifikats

Siehe Anhang A.

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 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 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 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.

Aktuell werden für die Rollenauthentisierung die Zugriffsprofile 0 bis 9 unterschieden. Die die Geräteauthentisierung 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-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.

Mit ihrer Registrierung erhält eine CVC-CA nur das Recht, CV-Zertifikate mit bestimmten Zugriffsprofilen zu erzeugen (siehe Abschnitt 5.2.1). Erzeugt eine CVC-CA CV-Zertifikate mit anderen Zugriffsprofilen als den bei ihrer Registrierung festgelegten, wird ihre Registrierung durch die gematik widerrufen (siehe Abschnitt 5.2.4). Eine Chipkarte, die bei ihrer Herstellung ein CV-Zertifkat mit einem nicht korrektem Zugriffsprofil erhalten hat, MUSS unverzüglich eingezogen werden (falls sie bereits ausgegeben wurde) und anschließend vernichtet werden.

4.5 Zuständigkeiten

An der PKI für CV-Zertifikate sind verschiedene Organisationen bzw. Personen beteiligt. In den folgenden Abschnitten wird ein Überblick über die vorhandenen Rollen (im Rahmen der PKI) und deren Zuständigkeiten bzw. Verantwortlichkeiten in Bezug auf die PKI für CV-Zertifikate gegeben.

Im Rahmen der Telematikinfrastruktur gibt es neben der PKI für CV-Zertifikate weitere PKI. Die im Folgenden genannten Rollen haben ggf. auch im Rahmen dieser weiteren PKI Zuständigkeiten und Verantwortlichkeiten. Hierauf wird im Folgenden jedoch nicht weiter eingegangen.

Bei der folgenden Beschreibung wird von einer Trennung der Organisationen bzw. Personen bei der Ausübung der Rollen ausgegangen. Eine Organisation bzw. Person kann jedoch mehrere Rollen übernehmen.

Übernimmt eine Organisation/Person eine Rolle, so kann sie Teile der zu dieser Rolle gehörenden Zuständigkeiten/Aufgaben an eine andere Organisation/Person übergeben. Hiervon unabhängig bleiben aber die im Folgenden genannten Verantwortlichkeiten bei der die Rolle ausübenden Organisation/Person.

4.5.1 gematik

Die gematik ist verantwortlich für die gesamte PKI der CV-Zertifikate. Sie übernimmt unter anderem die folgenden Aufgaben:

- Beauftragung und Kontrolle des Betreibers der Root-CVC-CA,
- Registrierung der CVC-CAs der zweiten Ebene,
- ggf. Widerruf der Registrierung einer CVC-CA der zweiten Ebene,
- bei Bedarf Kontrolle einer CVC-CA der zweiten Ebene,

- Vorgabe der Algorithmen und Schlüssellängen für das Generieren der CV-Zertifikate,
- Entscheidung über einen Schlüsselwechsel bei der Root-CVC-CA [gemPKI_CVCGK]

4.5.2 Betreiber Root-CVC-CA

Der Betreiber der Root-CVC-CA betreibt als technischer Dienstleister im Auftrage der gematik die folgenden CAs:

- Produktiv-Root-CVC-CA,
- Test-Root-CVC-CA

Mit diesen generiert die Root-CVC-CA die (Produktiv- bzw. Test-) CA-CV-Zertifikate für die CVC-CAs der zweiten Ebene. Dabei stellt sie sicher, dass

- ein CA-CV-Zertifikat nur für eine CVC-CA generiert, falls diese aktuell gültig durch die gematik registriert ist, und
- das Ausstellen eines CA-CV-Zertifkats gemäß den Vorgaben aus Kapitel 7 geschieht.

Nach Entscheidung und Aufforderung durch die gematik führt der Betreiber einen Wechsel für das Schlüsselpaar der Root-CVC-CA durch und erzeugt die zugehörigen Cross-CV-Zertifikate.

Der Betreiber der Root-CVC-CA veröffentlicht die aktuellen öffentlichen Schlüssel der Produktiv- und Test-Root-CVC-CA sowie evtl. vorhandene Cross-CV-Zertifikate.

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.

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

Eine CVC-CA ist für das Generieren der CV-Zertifikate für eine Chipkarte (eGK, HBA, SMC) zuständig. Die dabei einzuhaltenden Anforderungen werden durch dieses Dokument vorgegeben.

Eine CVC-CA muss bei der gematik registriert werden. Dabei ist insbesondere durch ein Sicherheitsgutachten nachzuweisen, dass die in diesem Dokument beschriebenen Mindestanforderungen durch die CVC-CA eingehalten werden.

Eine CVC-CA muss ein CA-CV-Zertifikat für ihr Schlüsselpaar bei der Root-CVC-CA beantragen. Dieses muss bei jedem eigenen Schlüsselwechsel und nach jedem Schlüsselwechsel bei der Root-CVC-CA wiederholt werden.

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

Falls CV-Rollen-Zertifikate erzeugt werden sollen, die ein Zugriffsprofil ungleich 0 enthalten (d.h. die für einen HBA bzw. eine SMC bestimmt sind), benötigt die CVC-CA hierfür eine Qualifizierung durch die zuständige berufsständische Organisation. Die Anforderungen an diese Qualifizierung werden durch die berufsständische Organisation geregelt. Die CVC-CA muss in ihrem Antrag auf Registrierung bei der gematik nachweisen, dass sie über die notwendigen Qualifizierungen verfügt.

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

4.5.5 Kartenhersteller

Im Rahmen der Produktion einer Chipkarte (eGK, HBA, SMC) müssen für die PKI der CV-Zertifikate die folgenden Werte in die Chipkarte eingebracht werden:

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

Es liegt in der Verantwortung des Kartenherstellers, dass hierbei die korrekten Werte in die Chipkarte eingebracht werden.

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

4.5.6 Karteninhaber (eGK)

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

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

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

Ein HBA enthält ein CV-Rollen-Zertifikat mit einem Zugriffsprofil ungleich 0. Das genaue Zugriffsprofil ist dabei abhängig von der Berufsgruppe, zu der der Karteninhaber des HBA (Leistungserbringer wie Arzt, Apotheker etc.) gehört. Durch eine C2C-Authentikation mit einer eGK erhält der HBA und damit sein Karteninhaber weitere (von dem genauen Zugriffsprofil abhängige) Zugriffsrechte auf die Daten der eGK.

Im Rahmen der PKI für CV-Zertifikate hat ein Inhaber eines HBA die Verpflichtung,

- jede Änderung seiner Zugehörigkeit zu der (für die Ausgabe seines HBA relevanten) Berufsgruppe sowie
- den Verlust seines HBA

unverzüglich zu melden. Konkrete Festlegungen hierzu werden durch die für die Ausgabe des HBA zuständige berufsständische Organisation geregelt.

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

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

4.5.8 Karteninhaber (SMC-K, SMC-RFID)

Eine SMC-K bzw. eine SMC-RFID enthält nur ein CV-Geräte-Zertifikat. 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.

Es MUSS noch geklärt werden, ob der Karteninhaber einer SMC-K bzw. einer SMC-RFID den Verlust dieser Chipkarten melden muss. Falls ja MUSS geklärt werden, wo dies gemeldet werden soll.

4.6 Unterscheidung Test-CVC-CA und Produktiv-CVC-CA

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

Der Betreiber der Root-CVC-CA stellt sowohl eine Produktiv-Root-CVC-CA als auch eine Test-Root-CVC-CA zur Verfügung. Die beiden Systeme werden technisch,

organisatorisch und betrieblich so getrennt, dass keine gegenseitige Beeinflussung und keine Verwechslung möglich sind.

Jeder Betreiber einer CVC-CA der zweiten Ebene muss neben einer Produktiv-CVC-CA ebenfalls eine Test-CVC-CA betreiben. Das Testsystem muss dabei von dem Produktivsystem technisch, organisatorisch und betrieblich so getrennt werden, dass keine gegenseitige Beeinflussung und keine Verwechslung möglich sind.

Das CA-CV-Zertifikat einer Produktiv-CVC-CA wird durch den Betreiber der Root-CVC-CA mit deren Produktiv-Root-CVC-CA erzeugt. Das CA-CV-Zertifikat einer Test-CVC-CA wird durch den Betreiber der Root-CVC-CA mit deren Test-Root-CVC-CA erzeugt.

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]:

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

Eine Test-CVC-CA muss ebenfalls bei der gematik registriert werden. Hierfür gibt es ein verkürztes Verfahren (siehe Abschnitt 5.3).

Im Allgemeinen können nur solche Betreiber eine Test-CVC-CA bei der gematik registrieren lassen, die kurzfristig auch eine Produktiv-CVC-CA bei der gematik registrieren lassen. Eine Ausnahme von dieser Regelung gibt es nur für die gematik selber, die eine Test-CVC-CA (gematik Testlabor) betreiben wird, aber keine Produktiv-CVC-CA.

Anmerkung: Die in [gemBetr_BK] für ein Produktivsystem beschriebene weitere Unterscheidung der Umgebungen Produktionsumgebung (PU), Produktionsreferenz-umgebung (PRU) und Produktionstestumgebung (PTU) wird weder für die Root-CVC-CA noch für eine CVC-CA der zweiten Ebene gefordert.

4.7 Prozesse bis zur Zertifikatserstellung

CV-Zertifikate für eine eGK, einen HBA bzw. eine SMC werden durch eine CVC-CA der zweiten Ebene erzeugt. Damit die CV-Zertifikate erfolgreich im Rahmen einer C2C-Authentikation eingesetzt werden können, benötigt die CVC-CA ein eigenes CA-CV-Zertifikat, das durch die Root-CVC-CA ausgestellt wird. Hierfür wiederum wird eine vorherige Registrierung der CVC-CA durch die gematik benötigt. Die folgende Abbildung zeigt die notwendige Zusammenarbeit zwischen der gematik, den berufsständischen Organisationen, dem Betreiber der Root-CVC-CA und den CVC-CAs der zweiten Ebene:

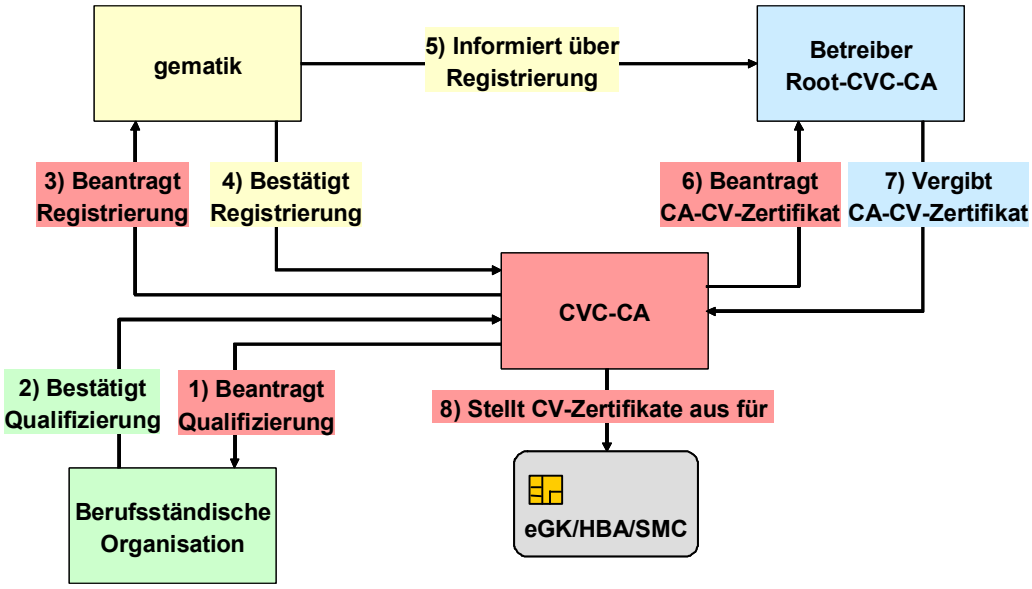

Abbildung 2 – Aufgabentrennung zwischen den an der CVC-PKI Beteiligten

Die Qualifizierung durch eine berufsständische Organisation wird nur benötigt, falls die CVC-CA CV-Rollen-Zertifikate mit einem Zugriffsprofil ungleich 0 für einen HBA bzw. eine SMC-A/SMC-B erzeugen will. Welche Qualifizierungen notwendig sind, wird durch den Kartenherausgeber des HBA bzw. der SMC-A/SMC-B vorgegeben. Anforderungen an die Durchführung der Qualifizierung werden durch die berufsständischen Organisationen festgelegt. Nachweise über das Vorliegen benötigter Qualifizierungen muss die CVC-CA ihrem Antrag auf Registrierung bei der gematik beilegen. Die Qualifizierungen müssen also vor der Beantragung der Registrierung abgeschlossen werden.

Die Prozesse für die Registrierung einer CVC-CA durch die gematik, eine ggf. notwendige Qualifizierung durch eine berufsständische Organisation und das Ausstellen eines CA-CV-Zertifikates für die CVC-CA durch die Root-CVC-CA werden für eine Produktiv-CVC-CA nur einmal (bzw. selten in größeren Abständen) ausgeführt.

Für eine Test-CVC-CA wird eine Qualifizierung durch eine berufsständige Organisation nicht benötigt. Ansonsten sind die Abhängigkeiten die gleichen wie bei einer Produktiv-CVC-CA.

4.8 Lebenszyklus eines CV-Zertifikats

4.8.1 Generierung eines CV-Zertifikats

CV-Zertifikate dürfen nur auf Antrag eines hierfür Berechtigten generiert werden. Hierbei gilt:

- Ein Antrag für ein CV-Zertifikat für eine CVC-CA darf nur durch den Betreiber der CVC-CA gestellt werden. Hierfür ist eine vorherige Registrierung der CVC-CA durch die gematik notwendig. Der Antrag muss direkt bei dem Betreiber der Root-CVC-CA gestellt werden. Details dieses Vorgangs werden in Kapitel 7 beschrieben.

- Ein Antrag für ein CV-Zertifikat für eine Chipkarte (eGK, HBA, SMC) darf nur durch den Herausgeber dieser Chipkarte bzw. durch einen durch den Herausgeber beauftragten Kartenhersteller gestellt werden. Der Antrag muss bei dem Betreiber der CVC-CA gestellt werden. Details dieses Vorgangs müssen zwischen Kartenherausgeber, CVC-CA und Kartenhersteller geregelt werden. Grundlegende Anforderungen hierzu siehe Abschnitt 6.5.

Bei der Generierung eines CV-Zertifikats müssen die Anforderungen aus Kapitel 6 eingehalten werden.

4.8.2 Einbringen CV-Zertifikat in die Chipkarte

Nach der Generierung muss das CV-Zertifikat in die zugehörige Chipkarte eingebracht werden. Die hierfür notwendigen Prozesse müssen bilateral zwischen der CVC-CA und dem Kartenhersteller festgelegt werden. Grundlegende Anforderungen hierzu siehe Abschnitt 6.5.

4.8.3 Veröffentlichung eines CV-Zertifikats

CV-Zertifikate werden im Allgemeinen[1] nicht veröffentlicht. Verzeichnisdienste für einen Download der CV-Zertifikate werden im Rahmen der PKI für CV-Zertifikate nicht zur Verfügung gestellt.

4.8.4 Sperrung eines CV-Zertifikats

CV-Zertifikate können 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.

4.8.6 Gültigkeitsabfragen

Entsprechend den Vorgaben in den Abschnitten 4.8.4 und 4.8.5 gibt es im Rahmen der PKI für CV-Zertifikate keine Dienste, die Anfragen bezüglich der Gültigkeit eines CV-Zertifikates beantworten.

[1] Abweichend hiervon veröffentlicht der Betreiber der Root-CVC-CA seine öffentlichen Schlüssel und ggf. nach einem Schlüsselwechsel [gemPKI-CVCGK] erstellte Cross-CV-Zertifikate.

5 Registrierung einer CVC-CA

Damit im Rahmen der Telematikinfrastruktur eine CVC-CA an der PKI für CV-Zertifikate teilnehmen kann, muss der Betreiber die CVC-CA bei der gematik registrieren lassen. Dabei wird zwischen der Registrierung einer Produktiv-CVC-CA und der Registrierung einer Test-CVC-CA unterschieden.

Mit dem Antrag auf Registrierung einer Produktiv-CVC-CA oder einer Test-CVC-CA akzeptiert der Betreiber alle Vorgaben und Regelungen dieses Dokuments.

5.1 Allgemeine Regelungen

5.1.1 Geltungsbereich

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

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

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.

5.1.2 Produktiv-/Test-CVC-CA

Bei der Registrierung einer CVC-CA wird zwischen der Registrierung für den Produktivbetrieb und der Registrierung für den Testbetrieb unterschieden. Wesentlicher Unterschied der beiden Verfahren ist, dass bei einer Registrierung für den Testbetrieb noch keine Gutachten über die Sicherheit der Test-CVC-CA bzw. eine Qualifizierung für die Ausgabe von HBAs/SMCs benötigt werden.

5.1.3 Registrierung/Widerruf

Eine Registrierung einer Produktiv- bzw. Test-CVC-CA wird auf Antrag des Betreibers durch die gematik durchgeführt.

Ein Widerruf einer vorher durchgeführten Registrierung durch die gematik ist möglich. In Frage kommende Gründe hierfür sind in den Abschnitten 5.2.4 und 5.3.3 beschrieben.

5.1.4 Information Betreiber der Root-CVC-CA

Die gematik informiert den Betreiber der Root-CVC-CA regelmäßig über die aktuell registrierten Produktiv- bzw. Test-CVC-CAs. Dies geschieht

- spätestens fünf Werktage nach einer erfolgreichen Registrierung einer CVC-CA bzw.
- spätestens einen Werktag nach dem Widerruf einer Registrierung.

5.1.5 Notwendigkeit der Registrierung

Die Root-CVC-CA wird ein CV-Zertifikat für eine Produktiv- bzw. Test-CVC-CA nur dann erzeugen, falls diese aktuell als Produktiv- bzw. Test-CVC-CA bei der gematik registriert ist. Eine Ausnahme hiervon ist nicht möglich.

5.1.6 Kosten des Verfahrens

Die Registrierung einer CVC-CA der zweiten Ebene durch die gematik ist kostenfrei.

5.2 Verfahren für eine Produktiv-CVC-CA

5.2.1 Antrag auf Registrierung

Für die Registrierung einer Produktiv-CVC-CA muss der Betreiber einen schriftlichen Antrag an die gematik stellen. Zu diesem Antrag gehören:

- vollständig ausgefülltes Formular "Antrag Registrierung Produktiv-CVC-CA",
- ausgefülltes Formular "Liste der Kontaktpersonen",
- Kopie des Registerauszugs,
- Sicherheitsgutachten (6.2),
- ggf. Qualifizierungsnachweise für HBAs/SMCs (6.3).

Bei akkreditierten CAs sind, anstelle des Sicherheitsgutachtens, folgende Unterlagen zwingend erforderlich:

- Kopie der Akkreditierungsurkunde,
- Kopie der Bestätigungsurkunde "Bestätigung für die Umsetzung von Sicherheitskonzepten".
- Selbsterklärung zur Einhaltung des Betriebs CVC unter akkreditierten Bedingungen.

In dem Formular "Antrag Registrierung Produktiv-CVC-CA" muss unter Firma/Organisation die Adresse der eigentlichen Betriebsstätte der Produktiv-CVC-CA angegeben werden.

In dem Formular "Liste der Kontaktpersonen" muss für die Rolle "Leiter CA" ein verantwortlicher Mitarbeiter und ein Stellvertreter genannt werden. Für die Rolle "Sicherheitsbeauftragter" muss ein verantwortlicher Mitarbeiter genannt werden, ein Stellvertreter ist optional. Für die Rolle "Antragsteller CA-CV-Zertifikat" können bis zu drei Mitarbeiter genannt werden.

Anmerkung: Bei dem späteren Ausstellen des (Produktiv-) CA-CV-Zertifikats muss einer der in dem Formular "Liste der Kontaktpersonen" genannten Mitarbeiter persönlich bei dem Betreiber der (Produktiv-) Root-CVC-CA erscheinen.

Die genannten Formulare sind als PDF-Formulare konzipiert. Sie können von der gematik-Website herunter geladen werden und sind elektronisch auszufüllen. Sie müssen (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 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 (6.1) 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 rechtsverbindlich nach Registerauszug unterschrieben sein.

5.2.2 Entscheidung über die Registrierung

Über eingehende Anträge auf Registrierung einer Produktiv-CVC-CA entscheidet die gematik innerhalb von fünfzehn Werktagen.

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,
- das Sicherheitsgutachten bestätigt, dass die Mindestanforderungen aus Abschnitt 6.6 durch den Betreiber erfüllt werden,
- bei akkreditierten CAs die notwendigen Unterlagen nach Abschnitt 5.2.1 vollständig vorliegen,

- die für die Profile der zu generierenden CV-Zertifikate benötigten Qualifizierungsnachweise vorliegen und
- keine sonstigen Gründe gegen die Registrierung sprechen.

Die Gültigkeit der Registrierung ist zeitlich beschränkt. Der Betreiber wird über die Registrierung und deren Gültigkeit informiert. Der Betreiber muss rechtzeitig vor Ablauf der Gültigkeit seiner Registrierung einen neuen Antrag bei der gematik stellen.

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 CVC-CA in ein anderes Land,
- Änderungen bei der Zuordnung von Mitarbeitern zu den Rollen "Leiter CA", "Sicherheitsbeauftragter" oder "Antragsteller CA-CV-Zertifikat",
- Änderungen an den in dem Sicherheitskonzept beschriebenen technischen, baulichen und organisatorischen Sicherheitsmaßnahmen bzw. bei deren Umsetzung innerhalb des Betriebs der CVC-CA,
- CV-Zertifikate zukünftig auch mit solchen Profilen (letztes Byte in dem Feld CHA) erzeugt werden sollen, die noch nicht in der Registrierung genannt wurden

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.

Liegen Änderungen vor, die für das Sicherheitskonzept relevant sind, muss der Änderungsmitteilung ein neues Sicherheitsgutachten beigefügt werden. Dieses Sicherheitsgutachten muss bestätigen, dass die Mindestanforderungen aus Abschnitt 6.6 auch nach den Änderungen erfüllt werden.

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.

5.2.4 Widerruf einer Registrierung

In den folgenden Fällen wird die Registrierung einer CVC-CA durch die gematik widerrufen:

- zeitlicher Ablauf der Gültigkeit der Registrierung, ohne dass rechtzeitig ein erneuter Antrag durch den Betreiber der CVC-CA gestellt wurde,
- Bekannt werden von Änderungen gemäß Abschnitt 5.2.3 ohne dass diese der gematik mit einer Änderungsmitteilung ordnungsgemäß durch den Betreiber mitgeteilt wurden,
- Bekannt werden von Sicherheitsproblemen/-verstößen bei der CVC-CA,
- Verlagerung des Hauptsitzes des Betreibers oder der eigentlichen Betriebsstätte der CVC-CA in ein Land außerhalb der Europäischen Union,
- Änderungsmitteilung gemäß Abschnitt 5.2.3 über eine für das Sicherheitskonzept relevante Änderung ohne entsprechender positiver Einschätzung durch ein Sicherheitsgutachten eines durch die gematik anerkannten Gutachters,
- Änderungsmitteilung gemäß Abschnitt 5.2.3 über die zukünftige Produktion von CV-Zertifikaten mit neuen Profilen ohne Einreichung entsprechender Qualifizierungsnachweise der für diese Profile zuständigen berufsständischen Organisationen.

Bei einem Widerruf der Registrierung ist der Betreiber der CVC-CA verpflichtet,

- unverzüglich die Produktion neuer CV-Zertifikate einzustellen,
- alle Schlüsselpaare, für die er ein CA-CV-Zertifikat der Root-CVC-CA besitzt, zu vernichten (siehe auch Abschnitt 6.6.4) und
- die Durchführung dieser Maßnahmen der gematik schriftlich zu bestätigen.

Die gematik informiert den Betreiber der Root-CVC-CA über den Widerruf der Registrierung. Die Root-CVC-CA wird danach keine CA-CV-Zertifikate mehr für die CVC-CA ausstellen. Dies gilt sowohl für die Produktiv- als auch die Test-CVC-CA.

Anmerkung: Für die CVC-CA durch die Root-CVC-CA ausgestellte CA-CV-Zertifikate sowie durch die CVC-CA ausgestellte CV-Zertifikate für eine Chipkarte (eGK, HBA, SMC) bleiben auch nach einem Widerruf der Registrierung der CVC-CA gültig. Eine Sperrung dieser Zertifikate ist im Rahmen der PKI für CV-Zertifikate nicht möglich. Die CVC-CA kann aber nach dem Widerruf ihrer Registrierung keine neuen CV-Zertifikate für Chipkarten generieren, da sie verpflichtet ist, ihre zugehörigen Schlüsselpaare zu vernichten.

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 Registrierung nachgewiesenen Sicherheitsbedingungen durchführt wird. Das

Formular muss vollständig ausgefüllt werden. Unter diesen Voraussetzungen kann das Schlüsselpaar weiter verwendet werden.

5.3 Verfahren für eine Test-CVC-CA

5.3.1 Antrag auf Registrierung

Für die Registrierung einer Test-CVC-CA muss der Betreiber einen schriftlichen Antrag an die gematik stellen. Zu diesem Antrag gehören:

- Vollständig ausgefülltes Formular "Antrag Registrierung Test-CVC-CA",
- Ausgefülltes Formular "Liste der Kontaktpersonen",
- Kopie des Registerauszugs

In dem Formular "Antrag Registrierung Test-CVC-CA" muss unter Firma/Organisation die Adresse der eigentlichen Betriebsstätte der Test-CVC-CA angegeben werden.

In dem Formular "Liste der Kontaktpersonen" muss für die Rollen "Leiter CA", "Sicherheitsbeauftragter" und "Antragsteller CA-CV-Zertifikat" jeweils mindestens eine Person genannt wird. Eine Person kann dabei für mehrere Rollen genannt werden.

Die beiden genannten Formulare sind als PDF-Formulare konzipiert. Sie können von der gematik-Website herunter geladen werden und sind elektronisch auszufüllen. Sie müssen (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.

Anmerkung: Bei dem späteren Ausstellen des (Test-) CA-CV-Zertifikats muss eine der in dem Formular "Liste der Kontaktpersonen" genannten Mitarbeiter persönlich bei dem Betreiber der (Test-) Root-CVC-CA erscheinen.

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 rechtsverbindlich nach Registerauszug unterschrieben sein.

5.3.2 Entscheidung über die Registrierung

Über eingehende Anträge auf Registrierung einer Test-CVC-CA entscheidet die gematik innerhalb von fünf Werktagen.

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

- der Antrag gemäß den Vorgaben in Abschnitt 5.3.1 vollständig ist und

- keine sonstigen Gründe gegen die Registrierung sprechen.

5.3.3 Widerruf der Registrierung

Eine einmal erfolgreich durchgeführte Registrierung einer Test-CVC-CA wird in den folgenden Fällen durch die gematik widerrufen:

- Einstellung des Betriebs,
- ein Jahr nach der Registrierung wurde noch keine erfolgreiche Registrierung der zugehörigen Produktiv-CVC-CA durchgeführt

Eine Ausnahme von dieser Regelung (Punkt 2) existiert für die Test-CVC-CA der gematik. Die gematik wird nur eine Test-CVC-CA betreiben, aber keine Produktiv-CVC-CA.

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.

6 Anforderungen an eine CVC-CA

Die in diesem Kapitel enthaltenen Anforderungen an eine CVC-CA sind Mindestanforderungen. Die Umsetzung dieser Mindestanforderungen ist eine notwendige Voraussetzung für die Registrierung einer CVC-CA durch die gematik. Die Umsetzung muss durch Vorlage eines Sicherheitsgutachtens nachgewiesen werden.

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

Kartenherausgeber können weitere (höhere) Anforderungen an eine CVC-CA stellen. Die Definition dieser weiteren Anforderungen und der Nachweis ihrer Umsetzung werden bilateral zwischen dem Kartenherausgeber und dem Betreiber der CVC-CA geregelt. Für die Registrierung der CVC-CA durch die gematik sind diese weiteren Anforderungen nicht relevant.

6.1 Anforderungen an das Sicherheitskonzept

Der Betreiber einer CVC-CA MUSS ein Sicherheitskonzept erstellen, das mindestens die folgenden Punkte enthält:

- Beschreibung aller technischen, baulichen und organisatorischen Sicherheitsmaßnahmen und Bewertung von deren Eignung,
- Übersicht über alle eingesetzten Produkte,
- Übersicht über die Aufbau- und Ablauforganisation,
- Beschreibung der Trennung von Produktiv- und Test-CVC-CA,
- Verfahren zur Beurteilung und Sicherstellung der Zuverlässigkeit des eingesetzten Personals,
- Abschätzung und Bewertung der verbleibenden Sicherheitsrisiken

Für die Bewertung der Eignung der Sicherheitsmaßnahmen ist von den Vorgaben für die Schutzbedarfsfeststellung aus Abschnitt 6.6.1 auszugehen.

Der Betreiber einer CVC-CA KANN sich bezüglich Umfang und Aufbaus seines Sicherheitskonzepts KÖNNEN an den Vorgaben für die Sicherheitskonzepte der Dienstebetreiber aus [gemSiKo#8.6] orientieren.

6.2 Sicherheitsgutachten

Für die Registrierung einer Produktiv-CVC-CA MUSS der Betreiber ein Sicherheitsgutachten vorlegen. In diesem Sicherheitsgutachten MÜSSEN die folgenden Punkte enthalten sein:

- Bewertung der Eignung der im Sicherheitskonzept beschriebenen Maßnahmen,
- Bewertung der Vollständigkeit der im Sicherheitskonzept beschriebenen Maßnahmen,
- Bewertung der im Sicherheitskonzept enthaltenen Restrisikobetrachtung,
- Zusammenfassung und Gesamturteil

Das Sicherheitsgutachten MUSS von einem durch die gematik anerkannten Gutachter erstellt werden. Die gematik veröffentlicht eine Liste mit anerkannten Gutachtern. Bereits beim Betreiber vorhandene Sicherheitsgutachten können durch die gematik anerkannt werden, falls diese für ein System des Betreibers mit vergleichbaren oder höheren Sicherheitsanforderungen erstellt wurden und die CVC-CA unter gleichen Bedingungen wie das begutachtete System betrieben wird. In diesem Falle ist dies durch eine entsprechende Selbsterklärung (siehe Abschnitt 5.2.1) zu bestätigen.

6.3 Anforderungen an eine HBA-/SMC-Qualifizierung

Falls eine CVC-CA CV-Zertifikate für einen HBA bzw. eine SMC erzeugt, benötigt sie hierfür eine entsprechende Qualifizierung durch die für die Herausgabe dieser Karten zuständige berufsständische Organisation. Ein Nachweis über diese Qualifizierung muss dem Antrag auf Registrierung einer Produktiv-CVC-CA beigefügt werden.

Eine berufsständische Organisation KANN an eine CVC-CA für die Ausgabe von CV-Zertifikaten mit bestimmten Zugriffsprofilen zusätzlich eigene Anforderungen stellen, die über die in diesem Dokument genannten Mindestanforderungen der gematik hinausgehen. Durch die Qualifizierung bestätigt die berufsständische Organisation, dass die CVC-CA diese zusätzlichen eigenen Anforderungen erfüllt.

Die Beschreibung zusätzlicher Anforderungen einer berufsständischen Organisation sowie Festlegungen zum Prozess der Qualifizierung einer CVC-CA liegen in der Verantwortung der jeweiligen Organisation. Mit einem Formular (siehe Kapitel 8) bestätigt die Organisation gegenüber der gematik, dass die Qualifizierung für die CVC-CA erfolgreich durchgeführt wurde. Im Rahmen der Registrierung überprüft die gematik das Vorhandensein der Qualifizierung und dass der Nachweis durch eine berechtigte Person unterzeichnet wurde. Inhaltliche Überprüfungen der Qualifizierung werden durch die gematik nicht durchgeführt. Im Vorfeld teilen die zuständigen berufsständischen Organisationen der gematik mit, welche ihrer Mitarbeiter zeichnungsberechtigt für die Nachweise sind.

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 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.

6.4 Haftung der CVC-CA

Alle Fragen bezüglich der Haftung für Fehler/Schäden, die durch den Betrieb der Root-CVC-CA entstehen, werden zwischen der gematik und dem Betreiber der Root-CVC-CA geregelt.

Alle Fragen bezüglich der Haftung für Fehler/Schäden, die durch den Betrieb einer CVC-CA entstehen, werden zwischen dem die CVC-CA beauftragenden Kartenherausgeber und dem Betreiber der CVC-CA geregelt.

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:

- Eine Chipkarte mit zugehörigem CV-Zertifikat darf nur im Auftrag eines berechtigten Kartenherausgebers produziert werden ([gemSiKo#B4.5.3]).
- In dem CV-Rollen-Zertifikat einer Chipkarte darf nur ein für den Karteninhaber der Chipkarte zugelassenes Zugriffprofil (Feld CHA) kodiert sein ([gemSiKo#B4.5.3]).
- In einem CV-Geräte-Zertifikat einer Chipkarte darf ein bestimmtes Zugriffsprofil nur dann kodiert sein, falls das Gerät, in dem diese Chipkarte eingebracht wird, auch diese Funktionseinheit unterstützt.
- In einem CV-Geräte-Zertifikat einer Chipkarte darf insbesondere nur dann das Zugriffsprofil 51 (Signaturanwendungskomponente SAK) kodiert sein, falls diese Chipkarte in einen Konnektor eingebracht wird, der eine Funktionseinheit Signaturanwendungskomponente gemäß SigG/SigV unterstützt.
- In dem CV-Zertifikat einer Chipkarte muss die korrekte ICCSN der Chipkarte (Feld CHR) kodiert sein ([gemSiKo#B4.5.3]).
- Nach Produktion MUSS in der Chipkarte der private Schlüssel enthalten sein, der zu dem durch das enthaltene CV-Zertifikat zertifizierten öffentlichen Schlüssel gehört ([gemSiKo#B4.5.3]).
- Die Sicherheit des privaten Schlüssels MUSS immer gewährleistet sein. Dieses bedeutet, dass der private Schlüssel in einem HSM generiert werden muss, nie außerhalb des HSM im Klartext vorhanden sein darf und nach der Personalisierung in die Chipkarte in allen anderen HSM gelöscht werden muss ([gemSiKo#F5.1]).

- 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]).
- 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]).
- Chipkarten, die vor Ausgabe an den Karteninhaber als fehlerhaft erkannt werden, müssen ordnungsgemäß vernichtet werden ([gemSiKo#B4.4.1]).
- Chipkarten, die fehlerfrei produziert wurden, müssen an den vorgesehenen Karteninhaber übergeben werden ([gemSiKo#B4.4.1]).

Die genannten Sicherheitsziele können nicht nur durch Sicherheitsmaßnahmen bei einem der an der Produktion beteiligten Organisationen erreicht werden. Es ist vielmehr eine zwischen den Beteiligten abgestimmte Zusammenarbeit verschiedener Sicherheitsmaßnahmen der beteiligten Organisationen notwendig. Aus Sicht der PKI für CV-Zertifikate ist die CVC-CA stellvertretend für alle Beteiligten für die Einhaltung der Anforderungen verantwortlich.

In dem Sicherheitskonzept der CVC-CA MUSS beschrieben werden, wie diese Zusammenarbeit organisiert ist und wie die entsprechenden Sicherheitsmaßnahmen bei den einzelnen Organisationen greifen.

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:

Objekt	Referenz
Privater Schlüssel Root-CVC-CA	[gemSiKo#C2.87]
Öffentlicher Schlüssel/CA-CV-Zertifikat Root-CVC-CA	[gemSiKo#C2.88]
Privater Schlüssel CVC-CA	[gemSiKo#C2.89]
Öffentlicher Schlüssel/CA-CV-Zertifikat CVC-CA	[gemSiKo#C2.90]
Privater Schlüssel eGK für C2C-Auth.	[gemSiKo#C2.59]
Öffentlicher Schlüssel/CV-Zertifikat eGK	[gemSiKo#C2.24]
Privater Schlüssel HBA für C2C-Auth.	[gemSiKo#C2.60]
Öffentlicher Schlüssel/CV-Zertifikat HBA	[gemSiKo#C2.27]

Objekt	Referenz
Privater Schlüssel SMC-A für C2C-Auth.	[gemSiKo#C2.65]
Öffentlicher Schlüssel/CV-Zertifikat SMC-A	[gemSiKo#C2.64]
Privater Schlüssel SMC-B für C2C-Auth.	[gemSiKo#C2.69]
Öffentlicher Schlüssel/CV-Zertifikat SMC-B	[gemSiKo#C2.68]
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.

6.6.2 Verfügbarkeit der CVC-CA

Anforderungen für die Verfügbarkeit der CVC-CA werden nicht vorgegeben. Entsprechende Vorgaben werden zwischen dem die CVC-CA beauftragenden Kartenherausgeber und dem Betreiber der CVC-CA geklärt

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 eingesetzt werden.

6.6.4 Verlust der Registrierung

Falls eine CVC-CA ihre Registrierung bei der gematik verliert, ist sie verpflichtet, alle Schlüsselpaare, für die sie ein CA-CV-Zertifikat der Root-CVC-CA besitzt, unverzüglich zu vernichten [gemSiKo#B4.5.3]. Dies muss durch eine der folgenden Maßnahmen realisiert werden:

- physisches Zerstören des HSM, in dem der private Schlüssel gespeichert ist (diese Maßnahme ist zwingend vorgeschrieben, falls das HSM keine der beiden folgenden Möglichkeiten unterstützt),
- physisches Löschen des privaten Schlüssels innerhalb des HSM (falls das HSM diese Funktionalität unterstützt),
- dauerhaftes Sperren aller möglichen Zugriffe auf den privaten Schlüssel innerhalb des HSM (falls das HSM diese Funktionalität unterstützt)

Der Betreiber der CVC-CA muss der gematik die Vernichtung aller Schlüsselpaare schriftlich innerhalb von fünf Werktagen nach Eingang der Benachrichtigung über den Widerruf der Registrierung bestätigen.

6.6.5 Sicherheit des Schlüsselpaares

Die CVC-CA muss für die Sicherheit des Schlüsselpaares ein HSM einsetzen. Dabei muss gelten ([gemSiKo#F5.1]):

- Das Schlüsselpaar der CVC-CA (zum Signieren von CV-Zertifikaten) muss in einem HSM generiert werden.
- Der private Schlüssel der CVC-CA darf das HSM nie in Klartext verlassen.
- Alle kryptographischen Berechnungen mit dem privaten Schlüssel der CVC-CA müssen innerhalb des HSM erfolgen.

Als HSM kann eine Chipkarte zum Einsatz kommen.

Falls notwendig kann aus Gründen der Hochverfügbarkeit bzw. hoher Performanzanforderungen (Möglichkeit zur Lastverteilung) ein HSM "geklont" werden, indem der private Schlüssel aus dem HSM (kryptographisch abgesichert) exportiert wird und in ein weiteres HSM importiert wird. Dabei müssen die folgenden Punkte berücksichtigt werden ([gemSiKo#B4.5.4]):

- Falls das Klonen eines HSM technisch möglich ist, muss der Vorgang in dem Sicherheitskonzept gesondert beschrieben und in dem Sicherheitsgutachten gesondert bewertet werden. Dabei müssen insbesondere die Maßnahmen für die Gewährleistung der Sicherheit des privaten Schlüssels als auch die (technischen und/oder organisatorischen) Maßnahmen für die Verhinderung des unautorisierten Erstellens von Klonen beschrieben (Sicherheitskonzept) und bewertet (Sicherheitsgutachten) werden.
- Das Klonen eines HSM darf nur durch zwei Mitarbeiter (Vier-Augen-Prinzip) möglich sein.
- Das Klonen eines HSM muss protokolliert werden.
- Zu jeder Zeit muss einfach nachvollziehbar sein, wie viele Klone des HSM existieren.
- Alle Klone eines HSM (d.h. alle HSM mit dem gleichen privaten Schlüssel) werden in Sinne dieses Dokuments logisch als ein HSM betrachtet, d.h. alle Anforderungen an ein HSM gelten für jeden Klon.
- Alle Klone eines HSM (d.h. alle HSM mit dem gleichen privaten Schlüssel) müssen in einem geschützten Bereich der Betriebsstätte eingesetzt werden (siehe 6.6.9).

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. 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.

In diesem Fall muss das Schlüsselpaar vernichtet werden. Dies muss durch eine der folgenden Maßnahmen realisiert werden ([gemSiKo#B4.5.3]):

- Physikalisches Zerstören des HSM (ggf. aller Klone), in dem der private Schlüssel gespeichert ist. Diese Maßnahme ist zwingend vorgeschrieben, falls das HSM keine der beiden folgenden Möglichkeiten unterstützt.
- Physikalisches Löschen des privaten Schlüssels innerhalb des HSM (ggf. innerhalb aller Klone), falls das HSM diese Funktionalität unterstützt.
- Dauerhaftes Sperren aller möglichen Zugriffe auf den privaten Schlüssel innerhalb des HSM (ggf. innerhalb aller Klone), falls das HSM diese Funktionalität unterstützt.

Folgende Funktionen des HSM dürfen nur nach einer Benutzerauthentikation zweier hierfür autorisierter Nutzer (Vier-Augen-Prinzip) möglich sein ([gemSiKo#B4.5.4]):

- Generieren eines neuen Schlüsselpaares,
- Berechnung einer Signatur mit dem privaten Schlüssel,
- (kryptographisch abgesicherter) Export des privaten Schlüssels,
- (kryptographisch abgesicherter) Import eines privaten Schlüssels,
- Löschen des privaten Schlüssels (falls dies durch das HSM unterstützt wird),
- Sperren der Zugriffe auf den privaten Schlüssel (falls dies durch das HSM unterstützt wird)

Das genaue Vorgehen bei der Benutzerauthentikation kann durch den Betreiber festgelegt werden. Sowohl eine Benutzerauthentikation direkt gegenüber dem HSM als auch gegenüber der das HSM nutzenden Anwendung sind denkbar. Sichergestellt werden muss dabei aber, dass das HSM nur nach erfolgter Benutzerauthentikation genutzt werden kann.

Bei der Beantragung und Generierung des CA-CV-Zertifikates muss die Authentizität des öffentlichen Schlüssels sichergestellt werden. Dazu muss

- ein Fingerprint über den öffentlichen Schlüssel in dem Antragsschreiben an die Root-CVC-CA übermittelt werden und

- ein mit dem privaten Schlüssel signierter (den öffentlichen Schlüssel enthaltenen) CVC-PKCS#10-Request[2] an die Root-CVC-CA übermittelt werden.

Die genauen Formate für den Fingerprint und den CVC-PKCS#10-Request werden durch den Betreiber der Root-CVC-CA vorgegeben.

6.6.6 Schlüssellängen, Algorithmen

Die Algorithmen und Schlüssellängen werden durch [gemSpec_Krypt#5.1.2] festgelegt.

Die gematik kann die Vorgaben für die Schlüssellänge und die Algorithmen aufgrund neuer Erkenntnisse bezüglich der Sicherheit bestimmter Schlüssellängen und Algorithmen ändern. Die gematik informiert alle registrierten CVC-CAs der zweiten Ebene über entsprechende Änderungen.

Im Falle der Änderung der Vorgaben durch die gematik ist eine CVC-CA verpflichtet, die neuen Vorgaben nach einer Übergangsfrist umzusetzen. Die CVC-CA muss hierzu ein neues Schlüsselpaar mit der erforderlichen Schlüssellänge generieren und für dieses ein neues CA-CV-Zertifikat bei der Root-CVC-CA beantragen. Nach Ablauf der Übergangsfrist dürfen nur noch das neue Schlüsselpaar und ggf. die neuen Algorithmen bei der Generierung von CV-Zertifikaten genutzt werden.

Die Übergangsfrist wird ebenfalls durch die gematik vorgegeben.

Kann eine CVC-CA die neuen Vorgaben nicht innerhalb der Übergangsfrist umsetzen, muss sie dies der gematik unverzüglich mitteilen. Die Registrierung der CVC-CA wird in diesem Falle durch die gematik widerrufen.

6.6.7 Protokollierung

Die Arbeit der CVC-CA muss revisionssicher protokolliert werden ([gemSiKo#B4.5.3]). Folgende Ereignisse sind dabei mindestens zu protokollieren:

- Generierung eines neuen Schlüsselpaares im HSM,
- Löschung eines privaten Schlüssels im HSM,
- Export des privaten Schlüssels,
- Import des privaten Schlüssels,
- Sperrung der Zugriffe auf einen privaten Schlüssel im HSM,
- Erzeugen eines CV-Zertifikats mit einem Profil ungleich 0[3],
- Erzeugen einer Menge von CV-Zertifikaten mit Profil 0[4]

Bei jedem Ereignis müssen die folgenden Werte protokolliert werden:

[2] Struktur und Aufbau werden in Kapitel 7.3.1 beschrieben.
[3] Ein CV-Zertifikat mit einem Profil ungleich 0 (d.h. bei dem das letzte Byte in dem Feld CHA einen Wert ungleich 0 hat) ist für einen HBA bzw. eine SMC bestimmt.
[4] Ein CV-Zertifikat mit einem Profil gleich 0 (d.h. bei dem das letzte Byte in dem Feld CHA den Wert 0 hat) ist für eine eGK bestimmt.

- Datum und Uhrzeit,
- Typ des Ereignisses,
- Namen der beiden Mitarbeiter der CVC-CA, die das HSM frei geschaltet haben.

Bei dem Erzeugen eines CV-Zertifikates mit einem Profil ungleich 0 müssen zusätzlich die folgenden Werte protokolliert werden:

- Name des zuständigen Kartenherausgebers,
- Inhalt der Felder CHR und CHA,
- das erstellte CV-Zertifikat selber

Bei dem Erzeugen eines CV-Zertifikates mit einem Profil gleich 0 müssen zusätzlich die folgenden Werte protokolliert werden:

- Name des zuständigen Kartenherausgebers,
- Anzahl der erzeugten CV-Zertifikate

Die Protokollierung bei dem Erzeugen von CV-Zertifikaten mit Profil gleich 0 sollte pro Bestellung/Produktionslauf geschehen. Wichtig ist dabei, dass nachträglich anhand der Protokolle nachvollzogen werden kann, wann wie viele CV-Zertifikate mit einem Profil gleich 0 für wen erzeugt wurden.

Alle Protokolldaten müssen bei ihrer Erstellung, Verarbeitung und Speicherung geeignet gegen mögliche Manipulationen geschützt werden.

Auf Antrag muss Vertretern der gematik Einblick in die Protokolle gewährt werden. Die Protokolldaten müssen dazu in einfach verständlicher Form interpretierbar sein.

6.6.8 Personelle Anforderungen

Die CVC-CA muss in ihrem Organisationskonzept (als Teil des Sicherheitskonzepts) mindestens die folgenden Rollen unterscheiden ([gemSiKo#B4.5.3]):

- Leiter CVC-CA,
- Sicherheitsbeauftragter CVC-CA,
- Antragsteller CA-CV-Zertifikat,
- Zertifizierer.

Die Rolle "Zertifizierer" ist dabei für das Generieren von CV-Zertifikaten für eGKs, HBAs bzw. SMCs zuständig. Die Rolle "Antragsteller CA-CV-Zertifikat" ist dagegen für das persönliche Überbringen des CVC-PKCS#10-Requests zur Root-CVC-CA zuständig. Die genauen Aufgaben der Rollen MÜSSEN in dem Sicherheitskonzept der CVC-CA beschrieben werden. Geklärt werden MUSS dabei, welche verschiedenen Rollen nicht durch eine einzelne Person ausgeübt werden dürfen (Rollenausschlussmatrix). Dargestellt werden MUSS insbesondere, welche Rolle das HSM für welche Funktion der CVC-CA nutzen kann.

Im Rahmen der Registrierung MUSS die CVC-CA der gematik die verantwortlichen Mitarbeiter für die Rollen "Leiter CVC-CA", "Sicherheitsbeauftragter CVC-CA" und "Antragsteller CA-CV-Zertifikat" mitteilen. Für die ersten beiden Rollen MUSS dabei auch ein Stellvertreter genannt werden. Für die Rolle "Antragsteller CA-CV-Zertifikat" können optional zwei weitere Mitarbeiter genannt werden. Änderungen an den Zuordnungen von Mitarbeitern zu diesen Rollen MÜSSEN der gematik genannt werden. Die Root-CVC-CA wird nur dann ein CA-CV-Zertifikat für die CVC-CA ausstellen, falls der CVC-PKCS#10-Request persönlich durch einen hierfür vorher genannten Mitarbeiter überbracht wird.

Durch die tatsächliche Zuordnung von Rollen zu Mitarbeitern DARF NICHT ermöglicht werden, dass eine einzelne Person zwei Rollen ausüben kann, die Zugriffe auf das HSM im Vier-Augen-Prinzip für diese einzelne Person ermöglicht.

Die CVC-CA ist verpflichtet, für jede der genannten Rollen nur solche Mitarbeiter einzusetzen, die nachweislich die Vorraussetzungen hinsichtlich Ausbildung, Qualifikation, Erfahrung und Zuverlässigkeit erfüllen.

6.6.9 Betriebliche Anforderungen

Das die CVC-CA realisierende Kernsystem (insbesondere das HSM) muss in einem geschützten Bereich der Betriebsstätte untergebracht sein ([gemSiKo#B4.5.3]). Für diesen Bereich muss gelten:

- Der Zugang zu diesem Bereich ist nur autorisierten Mitarbeitern möglich.
- Beim Zugang muss der Mitarbeiter eindeutig identifiziert werden (z.B. durch Nutzung einer individuellen Chipkarte oder eines individuellen Zugangscodes).
- Der Zugang zu diesem Bereich wird protokolliert.
- Alle Zugänge sind in geeigneter Weise gegen Einbruch gesichert.
- Ist kein berechtigter Mitarbeiter anwesend, wird der Bereich alarmüberwacht.
- Besuchern ist der Zugang nur in Begleitung autorisierter Mitarbeiter und nur zu notwendigen, im Sicherheitskonzept beschriebenen Zwecken erlaubt.

Eine CVC-CA kann verteilt in zwei geschützten Bereichen (z.B. Primärrechenzentrum und Ausweichrechenzentrum des Betreibers) betrieben werden. Falls dabei Klone eines HSM in zwei geschützten Bereichen zum Einsatz kommen, muss sichergestellt werden, dass dadurch die Sicherheit des privaten Schlüssels nicht verringert wird. Entsprechende Maßnahmen müssen einem solchen Fall gesondert in dem Sicherheitskonzept beschrieben und in dem Sicherheitsgutachten bewertet werden. Zu beachten sind hierbei besonders die Anforderungen an ein HSM aus Abschnitt 6.6.5.

Es muss verhindert werden, dass das HSM (bzw. ein Klon des HSM) aus einem der geschützten Bereiche unautorisiert entfernt wird.

Falls zur CVC-CA gehörende Arbeitsplatz-Rechner oder Systeme außerhalb des geschützten Bereichs Zugriffe auf das Kernsystem in dem geschützten Bereich haben, müssen

- alle Zugriffe über diese Arbeitsplatz-Rechner bzw. Systeme auf das Kernsystem sowie
- die Kommunikation zwischen den Arbeitsplatz-Rechnern, den Systemen und dem Kernsystem

geeignet gegen Manipulationen und unautorisierte Nutzung geschützt werden ([gemSiKo#B4.5.3]).

Ist die CVC-CA in ein Netzwerk eingebunden, muss sichergestellt werden ([gemSiKo#B4.5.3]), dass

- über das Netzwerk nicht auf die CVC-CA zugegriffen werden kann und dass
- keine Informationen der CVC-CA über das Netzwerk weitergegeben werden können.

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#G] bei dem Betrieb einer CVC-CA berücksichtigt werden.

7 Ausstellen eines CV-Zertifikats für eine CVC-CA

Nach der Registrierung kann eine CVC-CA für einen öffentlichen Schlüssel ein CA-CV-Zertifikat bei der Root-CVC-CA beantragen. Dieses geschieht in zwei Schritten:

- Der Betreiber der CVC-CA stellt einen schriftlichen Antrag bei der Root-CVC-CA. Als Antwort wird ihm ein Termin mitgeteilt, an dem der Mitarbeiter der CVC-CA das CA-CV-Zertifikat persönlich bei der Root-CVC-CA abholen kann.
- An dem genannten Termin MUSS ein Mitarbeiter den CVC-PKCS#10-Request persönlich an die Root-CVC-CA überbringen. Nach Bearbeitung erhält er das neue CA-CV-Zertifikat.

Das Vorgehen ist bei CV-Zertifikaten für die Produktiv-CVC-CA und für die Test-CVC-CA identisch. Der Betreiber der Root-CVC-CA wird für die Produktion des CA-CV-Zertifikates entsprechend seine Produktiv- oder Test-Root-CVC-CA einsetzen.

7.1 CA-Namen

Jede CVC-CA MUSS einen (innerhalb der CVC-CA für eine Kartengeneration (4.2)) eindeutigen CA-Namen (5 ASCII-Zeichen) verwenden. Dabei gilt:

- Bei einer in Deutschland betriebenen CVC-CA MUSS der CA-Name bei der hierfür durch den DIN beauftragten Registrierungsstelle (Fraunhofer Gesellschaft SIT) registriert sein. Bisherige Kennungen und Antragsformular stehen unter www.sit.fraunhofer.de . Diese CA-Namen beginnen mit den zwei Zeichen DE.
- Bei einer außerhalb Deutschlands betriebenen CVC-CA MUSS der CA-Name bei der jeweils zuständigen nationalen Registrierungsstelle registriert sein.
- Die CA-Namen für Test-CVC-CA und für Produktiv-CVC-CA MÜSSEN unterschiedlich sein. CA-Namen für Test-CVC-CA müssen ein X enthalten[5].
- Die Produktiv-Root-CVC-CA hat den CA-Namen DEZGW.
- Die Test-Root-CVC-CA hat den CA-Namen DEGXX.

Anmerkung: Hat ein Betreiber verschiedene CVC-CAs, mit denen er CV-Zertifikate für verschiedene Kartengenerationen erzeugt, so KÖNNEN diese CVC-CAs den gleichen CA-Namen haben. In diesem Fall MUSS aber über die Belegung des Feldes CAR (siehe Anhang A.2.2) sichergestellt werden, dass die erzeugten CV-Zertifikate eindeutig zugeordnet werden können.

[5] Mit Fraunhofer Gesellschaft SIT wurde folgende Regelung vereinbart: Für CAs, die bereits einen registrierten CA-Namen haben, ergibt sich der CA-Name für die zugehörige Test-CVC-CA dadurch, dass das letzte Zeichen durch X ersetzt wird (sofern dadurch kein Konflikt mit bereits registrierten CA-Namen entstehen).

7.2 Schriftlicher Antrag der CVC-CA

7.2.1 Inhalt des Antrags

Der Betreiber CVC-CA MUSS ein neues CA-CV-Zertifikat schriftlich bei der Root-CVC-CA beantragen. Ein entsprechendes Antragsformular befindet sich auf der Homepage des Betreibers (aktuell: www.d-trust.net). Dieser Antrag MUSS die folgenden Angaben enthalten:

- Name und Anschrift der CVC-CA,
- CA-Name im Zertifikat (5 ASCII-Zeichen),
- Name und Vorname einer Kontaktperson,
- Typ des gewünschten Zertifikats (Test-/Produktiv-CVC-CA),
- Fingerprint über den öffentlichen Schlüssel, für den das CA-CV-Zertifikat erzeugt werden soll,
- Datum des Antrags,
- Unterschriften zweier hierfür berechtigter Mitarbeiter des Betreibers der CVC-CA

Für die Erzeugung des Fingerprints über den öffentlichen Schlüssel muss der Hashalgorithmus SHA-2 verwendet werden. Der Hashwert MUSS dabei über die gleiche Struktur gerechnet werden wie sie für den öffentlichen Schlüssel in den späteren CVC-PKCS#10-Request eingestellt wird.

Tabelle 3: Beispiel für einen öffentlichen Schlüssel mit Exponent F4

TAG	Length	Value
'30'	'82 XX XX'	
'02'	'82 XX XX'	Modulus
'02'	'03'	'01 00 01'

Die Angaben zu "Name und Anschrift der CVC-CA" sowie "CA-Name im Zertifikat" MÜSSEN identisch sein zu den Angaben in der Registrierung bzw. der letzten Änderungsmitteilung.

Als Kontaktperson MUSS ein Mitarbeiter genannt werden, dem bei der Registrierung bzw. bei einer Änderungsmitteilung einer der Rollen "Leiter CA", "Sicherheitsbeauftragter" bzw. "Antragsteller CA-CV-Zertifikat" zugewiesen wurde.

Eine der Unterschriften MUSS von einem Mitarbeiter stammen, dem bei der Registrierung bzw. bei einer Änderungsmitteilung der Rollen "Leiter CA" zugewiesen wurde. Die zweite

Unterschrift MUSS von einem weiteren bei der Registrierung bzw. einer Änderungsmitteilung genannten Mitarbeiter stammen.

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.

7.3 Ausstellen des Zertifikats

7.3.1 CVC-PKCS#10-Request

Der Betreiber der CVC-CA MUSS über den öffentlichen Schlüssel einen CVC-PKCS#10-Request gemäß der Struktur nach [PKCS#10] erstellen. Dieser MUSS mit dem zugehörigen privaten Schlüssel signiert werden. Folgende Konkretisierungen zu [PKCS#10] MÜSSEN umgesetzt werden:

- Im Request-Feld `certificationRequestInfo` MUSS `version` den Wert 0 haben.
- Im Request-Feld `certificationRequestInfo` MUSS `subject` die notwendigen Inhalte des CV-Zertifikats enthalten. Für die Angabe der Attribute MÜSSEN die OIDs gemäß unten stehender Tabelle verwendet werden.
- Im RequestInfo-Feld `subjectPKInfo` MUSS `algorithm` den Verwendungszweck `rsaEncrytion` ([PKCS#1], OID 1.2.840.113549.1.1.1) angeben.

- Im Request-Feld `signatureAlgorithm` MUSS `algorithm` das Signaturverfahren `sha256WithRSAEncryption` ([PKCS#1], OID 1.2.840.113549.1.1.11) angeben.

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
}
```

Auf der folgenden Seite sind die OIDs der Attribute zwecks leichterer Verständlichkeit in tabellarische Ansicht mit Inhaltsbeschreibung dargestellt:

Tabelle 4:OID der Attribute im CVC-PKCS#10-Request

OID											Name bzw. Inhalt der OID	
1											iso	
	3										identified-organization	
		6									dod	
			1								internet	
				4							private	
					1						enterprise	

						4788					D-Trust GmbH
							4				CVC-Attributes
								1			CPI (Certificate Profile Identifier) (1 Byte hex)
								2			CHR (Certificate Holder Reference)
									1		CA-Name (5 Zeichen ASCII)
									2		Service Indicator (1 nibble hex)
									3		Discretionary Data (1 nibble hex)
									4		Algorithm Reference (1 Byte hex)
									5		Aktivierungsjahr (1 Byte hex)
								4			OID (7 Byte hex für CAs)

Anmerkung: Im Gegensatz zu den CA-CV-Zertifikaten für die Kartengeneration G0 ist das Attribut CHA in CA-CV-Zertifikaten in der CVC-PKI für die Kartengeneration G1 nicht mehr enthalten.

Die Werte für die angegebenen Attribute MÜSSEN vollständig im `subject` des `certificationRequestInfo` im Request enthalten sein. Vorgaben für die einzelnen Werte sind in Anhang A zusammengestellt.

Der Betreiber der CVC-CA ist für die Korrektheit der Werte in seinem CVC-PKCS#10-Request verantwortlich. Der Betreiber der Root-CVC-CA übernimmt die angegebenen Werte in das CV-Zertifikat. Er führt neben den in Abschnitt 7.3.2 genannten keine weiteren Überprüfungen durch.

Der signierte CVC-PKCS#10-Request MUSS durch einen dazu berechtigten Mitarbeiter der CVC-CA persönlich an die Root-CVC-CA überbracht werden. Der CVC-PKCS#10-Request MUSS dabei base-64 kodiert sein. Als Übertragungsmedium wird ein USB-Stick verwendet. Bei Bedarf können weitere Übertragungsmedien bilateral zwischen dem Betreiber der Root-CVC-CA und der CVC-CA abgestimmt werden.

7.3.2 Vorgehen Root-CVC-CA

Erscheint ein Mitarbeiter einer CVC-CA mit einem CVC-PKCS#10-Request bei der Root-CVC-CA, führt diese die folgenden Überprüfungen durch:

- Liegt ein zugehöriger und durch die Root-CVC-CA bestätigter schriftlicher Antrag (siehe 7.1) vor?
- Liegt für die CVC-CA eine aktuell gültige Registrierung als Produktiv- bzw. Test-CVC-CA vor?
- Die Identität des erschienenen Mitarbeiters der CVC-CA wird anhand eines offiziellen Ausweisdokuments überprüft.
- Ist der erschienene Mitarbeiter in den Registrierungsdaten enthalten?
- Ist das mitgeführte Medium fehler- und virenfrei?

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

Hat eine der Überprüfungen ein negatives Ergebnis, wird der Vorgang abgebrochen.

Haben diese Überprüfungen ein positives Ergebnis, wird der CVC-PKCS#10-Request wie folgt überprüft:

- Stimmt der im Request-Feld `certificationRequestInfo` in `subject` enthaltene CA-Name mit dem CA-Namen aus dem schriftlichen Antrag überein?
- Über den in dem CVC-PKCS#10-Request enthaltenen öffentlichen Schlüssel wird ein (SHA-256) Fingerprint gerechnet. Stimmt dieser mit dem Fingerprint in dem schriftlichen Antrag überein?
- Kann die Signatur über den CVC-PKCS#10-Request verifiziert werden?

Hat eine der Überprüfungen ein negatives Ergebnis, wird der Vorgang abgebrochen.

Haben diese Überprüfungen ein positives Ergebnis, erzeugt die Root-CVC-CA das CV-Zertifikat für die CVC-CA. Dabei kommt wie in dem schriftlichen Antrag angegeben entweder die Produktiv- oder die Test-Root-CVC-CA zum Einsatz.

Das erzeugte CV-Zertifikat wird auf das Übertragungsmedium geschrieben, mit dem auch der CVC-PKCS#10-Request übertragen wurde. Das Zertifikat ist dabei DER-kodiert. Die Zertifikatsdatei enthält dabei neben dem eigentlichen CV-Zertifikat auch bereits die Angaben zu TAG und Length für die Speicherung des Zertifikats in dem EF der Chipkarte gemäß [gemSpec_eGK_P1#8.1.3].

8 Vorgaben Formulare

Die Formulare zur Beantragung der Registrierung als CVC-CA werden von der gematik bereitgestellt.

Sie sind als PDF-Formulare konzipiert und sind elektronisch auszufüllen. Sie müssen (direkt aus dem Formular heraus) ausgefüllt per Mail vorab an die gematik gesendet werden. Der mit dem Mailversand erstellte Ausdruck ist dann mit den restlichen benötigten Unterlagen per Post zu senden.

Alle Formulare des Antrages und die beigefügten Unterlagen müssen rechtsverbindlich nach Registerauszug (oder entsprechend vorgelegter Vertretungsvollmacht) unterschrieben sein.

Anhang A: Vorgaben für die CV-Zertifikate

A.1 – Aufbau und Berechnung eines CV-Zertifikats (informativ)

CV-Zertifikate können im Gegensatz zu X.509-Zertifikaten durch eine Chipkarte intern ausgewertet und überprüft werden. In Rahmen der Telematikinfrastruktur werden nur "nicht selbstbeschreibende" CV-Zertifikate mit einer Signatur mit "Message Recovery" verwendet.

Der Aufbau der CV-Zertifikate und ihre Berechnung werden für Chipkarten der Generation G1 durch [gemSpec_eGK _P1#8.1] normativ vorgegeben. Im Folgenden wird der Inhalt eines CV-Zertifikats für das Verständnis der folgenden Abschnitte informativ zusammengefasst.

Anmerkung: Die Berechnung der CV-Zertifikate gemäß [gemSpec_eGK_P1] ab Version 2.0.0 gilt für Chipkarten der Generation G1. Diese Berechnung eines CV-Zertifikats weicht stark ab von der Berechnung eines CV-Zertifikats gemäß älteren Versionen der Spezifikation [gemSpec_eGK_P1]. Für Chipkarten der Generation G0, die basierend auf älteren Versionen von [gemSpec_eGK_P1] realisiert werden, müssen die benötigten CV-Zertifikate weiterhin gemäß den Vorschriften der älteren Version von [gemSpec_eGK_P1] berechnet werden.

Die Signatur für ein CV-Zertifikat wird über eine Nachricht bestehend aus verschiedenen Feldern berechnet. Die Felder werden dabei ohne weitere Strukturinformationen oder Trennzeichen konkateniert. Welche Felder in welcher Reihenfolge zu der zu signierenden Nachricht zusammengefügt werden müssen, hängt dabei davon ab, ob das CV-Zertifikat für eine CVC-CA oder für eine Chipkarte erzeugt wird.

Berechnung eines CV-Zertifikats für eine CVC-CA über:

Tabelle 5: Informationen für ein CV-Zertifikat einer CVC-CA

CPI	Modulus	öffentlicher Exponent	OID	CHR	CAR	

Berechnung eines CV-Zertifikat für eine Chipkarte (eGK, HBA, SMC) über:

Tabelle 6: Informationen für ein CV-Zertifikat einer Chipkarte

CPI	Modulus	öffentlicher Exponent	OID	CHA	CHR	CAR

Die einzelnen Felder haben dabei folgenden Inhalt:

Tabelle 7: Übersicht Felder eines CV-Zertifikats

Feld	Inhalt
CPI	Certificate Profile Identifier: Dieser legt die genaue Struktur der Nachricht fest, über die die Signatur berechnet wird.

Feld	Inhalt
Modulus	Modulus des öffentlichen Schlüssels, für den das CV-Zertifikat berechnet wird.
öffentlicher Exponent	Öffentlicher Exponent des öffentlichen Schlüssels, für den das CV-Zertifikat berechnet wird.
OID	OID des Algorithmus, mit dem der private Schlüssel des Zertifikatsinhabers (CVC-CA oder Chipkarte) genutzt werden kann.
CHA	Certificate Holder Authorisation: Legt die Rolle des Zertifikatsinhabers fest.
CHR	Certificate Holder Reference: Eindeutiger Bezeichner des Schlüsselpaares des Zertifikatsinhabers, dessen öffentlichen Schlüssel in dem CV-Zertifikat enthalten ist.
CAR	Certification Authority Reference: Eindeutiger Bezeichner des Schlüsselpaares, mit dessen privaten Schlüssel die CVC-CA das CV-Zertifkat erzeugt hat.

A.2 – Vorgaben für einzelne Felder eines CV-Zertifikats

A.2.1 – Vorgaben der Kartenbetriebssysteme (informativ)

Die folgenden Felder eines CV-Zertifikats müssen durch das Betriebssystem einer Chipkarte intern 'verstanden' werden:

- CPI
- OID

Die gematik-Vorgaben für diese Betriebssysteme schränken daher die möglichen Werte für diese Felder wie folgt ein:

CPI identifiziert die Struktur des CV-Zertifikats. [gemSpec_eGK_P1#8.1] legt folgende Werte fest:

Tabelle 8: Mögliche Werte für CPI

CV-Zertifikat für	Wert für CPI
CVC-CA	'21'
Chipkarte	'22'

Die Angabe unter OID identifiziert den Verwendungszweck (Algorithmus) für das zugehörende Schlüsselpaar. [gemSpec_Krypt#5.1.2] und [gemSpec_eGK_P1#8.1] legen folgende Werte fest:

Tabelle 9: Mögliche Werte für OID

CV-Zertifikat für	Algorithmus	Wert für OID	Kodierung
CVC-CA	sigS_ISO9796-2 Withrsa_sha256	{1 3 36 3 4 2 2 4}	'2B 24 03 04 02 02 04'
Chipkarte	authS_ISO9796-2 Withrsa_sha256_mutual	{1 3 36 3 5 2 4}	'2B 24 03 05 02 04'

A.2.2 – Zusätzliche Vorgaben dieser Spezifikation (normativ)

Die folgenden Felder eines CV-Zertifikats werden durch das Betriebssystem einer Chipkarte nicht intern ausgewertet:

- CAR
- CHR
- CHA

Die genaue Festlegung für die Werte dieser Felder ist daher für die Spezifikation der Betriebssysteme nicht relevant. Damit übergeordnete Vorgaben der PKI jedoch umgesetzt werden können (z. B. die eindeutige Zuordnung eines CV-Zertifikats zu einem Schlüsselpaar), MÜSSEN auch für diese Felder Festlegungen zu den möglichen Werten getroffen werden. Die normativen Vorgaben für diese Felder werden im Folgenden beschrieben:

CAR

Das Feld CAR ist 8 Bytes lang und wie folgt weiter unterteilt:

Tabelle 10: Aufbau CAR

CA Name	Service-Indikator	CA-spezifische Information	Algortihmen-referenz	Datum

Folgende Festlegungen gelten:

- CA Name ist 5 Byte lang. Es MUSS der CA Name (siehe Abschnitt 7.1) eingetragen werden.
- Service-Indikator ist eine Ziffer (BCD-kodiert). Mögliche Werte siehe unten.
- CA-spezifische Information ist eine Ziffer (BCD-kodiert). Mögliche Werte siehe unten.
- Algorithmenreferenz sind zwei Ziffern (BCD-kodiert). Mögliche Werte siehe unten.
- Datum sind zwei Ziffern (BCD-kodiert). Es MÜSSEN die beiden letzten Ziffern des Jahres eingetragen werden, in dem das zugehörige Schlüsselpaar durch die CA aktiviert wurde.

Die Werte für Service-Indikator, CA-spezifische Information und Algorithmenreferenz kann der Betreiber der CA selber festlegen. Er MUSS dabei aber sicherstellen, dass die Zuordnung zwischen CAR und Schlüsselpaar eindeutig ist.

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. 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 bzw. für eine

- Authentisierung eines Gerätes.

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 weist eine Chipkarte nach einer C2C-Authentikation mit dem CV-Zertifikat gegenüber der anderen Karte nach, dass sie zu einem bestimmten Gerätetyp gehört.

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.
- 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.

A.3.1 – Rollenauthentisierung (informativ)

Aktuell werden die Zugriffsprofile 0 – 9 für eine Rollenauthentisierung unterschieden:

Tabelle 13: Zugriffsprofile für eine Rollenauthentisierung

Profil	Kodierung	CV-Zertifikate für
0	'00'	eGK
1 - 9	'01' – '09'	Rolle Zertifikatsinhaber bei HBA bzw. SMC-A
0 - 9	'00' – '09'	Rolle Zertifikatsinhaber bei SMC-B

Anmerkung: Es MUSS sichergestellt werden, dass bei einem HBA bzw. einer SMC-A/ SMC-B das Zugriffsprofil in einem CV-Zertifikat der Rolle des Karteninhabers bzw. der Organisation entspricht. Die Zuordnung der Profile zu den einzelnen Berufsgruppen bzw. Organisationen der Leistungserbringer ist nicht Gegenstand dieses Dokuments.

A.3.2 – Geräteauthentisierung (normativ)

Aktuell werden die Zugriffsprofile 51 – 55 für eine Geräteauthentisierung unterschieden:

Tabelle 14: Zugriffsprofile für eine Geräteauthentisierung

Profil	Kodierung	CV-Zertifikate für
51	'33'	SMC-K
52	'34'	SMC-RFID

53	'35'	HBA
54	'36'	SMC-A
55	'37'	SMC-B

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

Anhang B

B1 – Abkürzungen

Kürzel	Erläuterung
C2C	card to card
CA	certification authority
CHA	Certificate Holder Authorization
CHR	Certificate Holder Reference
CPI	Certificate Profile Identifier
CV	card verifiable
CVC	card verifiable certificate
CVC-CA	CA der zweiten Ebene der PKI für CV-Zertifikate
eGK	Elektronische Gesundheitskarte
HBA	Heilberufeausweis
HPC	Oberbegriff für HBA
HSM	Hochsicherheitsmodul
SigG	Signaturgesetz
SigV	Signaturverordnung
SMC	security module card
Root-CVC-CA	CA der obersten Ebene der PKI für CV-Zertifikate
ZDA	Zertifizierungsdienstleistungsanbieter (in diesem Dokument nur genutzt, falls qualifizierte (X.509-) Zertifikate ausgegeben werden)

B2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

B3 – Abbildungsverzeichnis

B4 – Tabellenverzeichnis

B5 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI]	BSI (12.2005): BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 1.0
[gemBetr_BK]	gematik (2007): Einführung der Gesundheitskarte – Betriebskonzept (nicht öffentlich)
[gemPKI_CVCGK]	gematik (19.03.2008): Einführung der Gesundheitskarte - Grobkonzept PKI für CV-Zertifikate V1.4.0
[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 V2.2.0
[gemSpec_eGK_P2]	gematik (25.03.2008): Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte ; Teil 2 – Grundlegende Applikationen V2.2.0
[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)

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	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 Applications and Functions Version 2.x.x
[HPC-P3]	Bundesärztekammer et al. (in Vorbereitung): German Health Professional Card and Security Module Card Part 3: SMC Applications and Functions Version 2.x.x
[PKCS#1]	RSA Laboratories (14.06.2002): PKCS #1 v2.1: RSA Cryptography Standard (www.rsasecurity.com/rsalabs)
[PKCS#10]	RSA Laboratories (26.05.2000): PKCS #10 v1.7: Certification Request Syntax Standard (www.rsasecurity.com/rsalabs)

B6 - Klärungsbedarf

Kap.	Offener Punkt	Zuständig
4.5.8	Es MUSS noch geklärt werden, ob der Karteninhaber einer SMC-K bzw. einer SMC-RFID den Verlust dieser Chipkarten melden muss. Falls ja MUSS geklärt werden, wo dies gemeldet werden soll	SPE/ZD SPE/DI