Einführung der Gesundheitskarte

Personalisierung kryptographischer Daten der eGK

Version:	1.0.0
Stand:	20.12.2006
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemPers_krypt]	gematik (20.12.2006): Einführung der Gesundheitskarte - Personalisierung kryptographischer Daten der eGK V1.0.0

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	13.09.06	Alle	Basisversion	gematik, AG3
0.0.2	04.10.06	Alle	Überarbeitet nach gematik-interner QS	gematik, AG3
0.0.3	25.10.06	alle	Überarbeitet nach weiteren Abstimmungen	gematik, AG3
0.0.4	26.10.06		Freigabe zur Vorkommentierung	gematik
0.9.1	18.12.06	4.1	Einarbeitung Ergebnisse aus der Vorkom-mentierung	gematik, AG3
1.0.0	20.12.06		Freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Bei der Personalisierung einer eGK werden nicht nur Versichertendaten in die eGK eingebracht, sondern auch kryptographische Daten. Diese kryptographischen Daten sind für das Funktionieren einer eGK im Rahmen der Telematikinfrastruktur notwendig. Die Sicherheit dieser Daten ist eine wesentliche Voraussetzung für die Sicherheit der gesamten Telematikinfrastruktur.

Die Sicherheit der kryptographischen Daten muss durch alle an der Personalisierung einer eGK beteiligten Organisationen gewährleistet werden. In diesem Dokument wird hierfür ein Mindestniveau für diese Sicherheit festgelegt. Die zugehörigen Sicherheitsanforderungen beziehen sich dabei nicht nur auf die Verarbeitung der kryptographischen Daten durch eine Organisation, sondern auch auf den Transport dieser Daten zwischen den beteiligten Organisationen. Das definierte Mindestniveau für die Sicherheit ist verpflichtend für alle beteiligten Organisationen. Die für das Einhalten des Mindestniveaus getroffenen Maßnahmen müssen in einem Sicherheitskonzept dokumentiert werden und durch ein Sicherheitsgutachten bewertet werden.

In [gemPers] wird eine Übergabeschnittstelle spezifiziert, über die Auftragsdaten und Rückmeldedaten eines Personalisierungsauftrags zwischen dem CMS des Kartenherausgebers und dem Personalisierer ausgetauscht werden können. Die Nutzung dieser Standardschnittstelle ist nicht verpflichtend, wird aber durch die gematik empfohlen. Die Schnittstelle enthält Vorkehrungen für die kryptographische Absicherung der zu übertragenden kryptographischen Daten einer eGK während des Transports. Diese Vorkehrungen und ihr Einsatz bei der Absicherung der kryptographischen Daten werden in diesem Dokument näher erläutert und müssen auch bei der Nutzung anderer Schnittstellen als der Standardschnittstelle zwingend eingehalten werden..

Für die genaue Organisation der Zusammenarbeit zwischen den an der Personalisierung einer eGK Beteiligten sind verschiedene Modelle denkbar. Die Schnittstelle aus [gemPers] kann dabei unabhängig von den konkreten Festlegungen für diese Zusammenarbeit genutzt werden. Bezüglich der kryptographischen Absicherung der Daten bei ihrem Transport kann es Abweichungen geben, die aber nicht zur Verletzung der definierten Sicherheitsvorgaben führen dürfen. Für drei verschiedene Organisationsmodelle wird in diesem Dokument aufgezeigt, welche Besonderheiten bei der Nutzung der Schnittstelle bezüglich der kryptographischen Absicherung berücksichtigt werden müssen.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Eine eGK enthält verschiedene kryptographische Daten. Diese müssen neben weiteren Versichertendaten während der Personalisierung in die eGK eingebracht werden. Generiert werden können die kryptographischen Daten dabei sowohl durch den Kartenherausgeber oder durch den Personalisierer als auch durch einen (durch den Kartenherausgeber bzw. Personalisierer beauftragten) Zulieferer. Kapitel 3 dieses Dokuments enthält eine Übersicht über die in einer eGK gemäß [gemSpec eGK-P2] vorhandenen kryptographischen Daten.

Die Sicherheit der kryptographischen Daten ist eine notwendige Voraussetzung für die Sicherheit der gesamten Telematikinfrastruktur. Bei der Verarbeitung von kryptographischen Daten müssen daher besondere Sicherheitsanforderungen erfüllt werden. Dies gilt für alle Organisationen, die von der Generierung eines solchen Datums bis zu seiner Personalisierung in eine eGK mit diesem Datum "in Berührung" kommen. Dieses Dokument stellt in Kapitel 4 die Anforderungen zusammen, die das notwendige Mindestniveau für die Sicherheit bei der Verarbeitung der kryptographischen Daten festlegen, das von allen Organisationen verpflichtend eingehalten werden muss.

Kryptographische Daten können als Teil der Personalisierungsauftragsdaten von dem CMS des Kartenherausgebers an den Personalisierer übertragen werden. Abhängig von der Zusammenarbeit zwischen Kartenherausgeber und Personalisierer können diese Daten aber auch als Teil der zugehörigen Rückmeldedaten von dem Personalisierer an das CMS übertragen werden. In beiden Fällen müssen die kryptographischen Daten bei ihrer Übertragung selber wieder kryptographisch abgesichert werden. In Kapitel 5 wird beschrieben, wie die hierfür vorgesehenen Teile der durch [gemPers] definierten Übertragungsschnittstelle zwischen dem CMS und dem Personalisierer genutzt werden können. Private Schlüssel aus RSA-Schlüsselpaaren dürfen in keinem Fall nach Abschluss des Produktionsprozesses außerhalb der jeweiligen eGK existieren; der Erzeuger dieser Schlüssel muss schlüssig beweisen können, dass er diese Schlüssel nach Einbringen in die eGK nicht mehr gespeichert hat (siehe hierzu Abschnitt 4.1.2).

An der Personalisierung einer eGK können neben dem Kartenherausgeber und dem Personalisierer verschiedene Zulieferer beteiligt sein. Die genaue Organisation der Zusammenarbeit der Beteiligten bei der Produktion einer eGK muss zwischen diesen bilateral geregelt werden. Kapitel 6 dieses Dokuments beschreibt, welche Aufgaben eine Organisation in Bezug auf die Sicherheit der kryptographischen Daten hat. Die jeweils gewählte Form der Zusammenarbeit muss von der gematik zugelassen werden und die von der gematik geforderten Sicherheitsvorgaben erfüllen. Dabei werden drei unterschiedliche Modelle für die Organisation der Zusammenarbeit betrachtet.

2.2 Zielgruppe

Dieses Dokument richtet sich an alle Organisationen, die direkt bzw. indirekt an der Personalisierung einer eGK beteiligt sind. Dazu gehören in erster Linie die

Kartenherausgeber (Betreiber eines CMS) und die eigentlichen Personalisierer, darüber hinaus aber auch alle Zulieferer/Erzeuger kryptographischer Daten einer eGK.

2.3 Geltungsbereich

Die in diesem Dokument enthaltenen Sicherheitsanforderungen an den Umgang mit kryptographischen Daten stellen ein Mindestniveau dar, das verpflichtend durch alle an der Personalisierung einer eGK direkt bzw. indirekt beteiligten Organisationen erfüllt werden muss.

Darüber hinaus empfiehlt die gematik, für den Austausch der Personalisierungsdaten zwischen dem CMS (des Kartenherausgebers) und dem Personalisierer die durch [gemPers] beschriebene standardisierte Schnittstelle für die Auftragsdaten und Rückmeldedaten zu verwenden und dabei bezüglich der Absicherung der zu übertragenden kryptographischen Daten die Vorgaben aus diesem Dokument zu verwenden.

2.4 Arbeitsgrundlagen

Die in diesem Dokument betrachteten kryptographischen Daten orientieren sich an der aktuellen Version von [gemSpec eGK-P2].

Die durch dieses Dokument beschriebenen Sicherheitsanforderungen orientieren sich an den Vorgaben aus dem gematik Sicherheitskonzept, den gematik Anforderungen für die PKI für CV-Zertifikate ([gemPKI-CVCGK], [gemPKI-Reg]) und den gematik Anforderungen an die PKI für X.509 Zertifikate [gemTSL-SP_CP].

2.5 Abgrenzung des Dokumentes

Bezüglich der Sicherheitsanforderungen stellt dieses Dokument eine Ergänzung und Präzisierung der Anforderungen aus dem gematik Sicherheitskonzept, den gematik Anforderungen für die PKI für CV-Zertifikate ([gemPKI-CVCGK], [gemPKI-Reg]), den gematik Anforderungen an die PKI für X.509 Zertifikate [gemTSL-SP_CP] und der TSL-Liste [gemX.509-TSL] dar. Bei ggf. vorhandenen Abweichungen gelten die Bestimmungen der Ausgangsdokumente.

3 Kryptographische Daten und Sicherheitsanforderungen

3.1 Vorhandene kryptographische Daten

Kryptographische Daten im Sinne dieses Dokumentes sind geheime Schlüssel, PINs/PUKs und die ggf. vorhandenen öffentlichen Schlüssel und Zertifikate.

Eine eGK enthält eine Anwendung QES für das Erzeugen qualifizierter elektronischer Signaturen. Für diese Anwendung enthält eine eGK verschiedene kryptographische Daten. Bei der Erzeugung, der Personalisierung bzw. dem Nachladen dieser Daten müssen verschiedene Anforderungen des SigG erfüllt werden. Verantwortlich hierfür ist in jedem Fall der ZDA, der das qualifizierte Zertifikat erzeugt. Die zu der Anwendung QES gehörenden kryptographischen Daten werden daher in diesem Dokument nicht weiter behandelt. Die zum Nachladen der qualifizierten elektronischen Signatur benötigten Vertrauensanker müssen schon bei der Personalisierung der Karten eingebracht werden. Alle Regelungen für diese Daten müssen durch den beteiligten ZDA in Abstimmung mit der gematik vorgegeben werden.

Bei der Nutzung einer eGK können (außerhalb der Anwendung QES) die in Tabelle 1 aufgeführten geheimen kryptographischen Daten (Schlüssel und PINs/PUKs) zum Personalisierer übertragen werden.

Die sichere Handhabung der privaten Schlüssel der CVC-CA zur Signatur des CV-Zertifikates werden im Dokument [gemPKI-Reg] und die Handhabung der privaten Schlüssel der X.509-CA in Dokument [gemTSL-SP_CP] beschrieben.

Tabelle 1 – Übersicht der zur Personalisierung der eGK übertragenen geheimen kryprographische Daten

Bezeichner	Typ	Gespeichert in	Nutzung für
KGK.CAMS.AUT KGK.CAMS.ENC	Masterschlüssel symmetrisch	CAMS	Ableiten der kartenindividuellen Schlüssel SK.CAMS.AUT und SK.CAMS.ENC
SK.CAMS.AUT SK.CAMS.ENC	kartenindividuell symmetrisch	CAMS(*) eGK	Authentikation zwischen eGK und CAMS (inkl. Aushandlung Session-schlüssel)
KGK.VSDD.AUT KGK.VSDD.ENC	Masterschlüssel symmetrisch	VSDD	Ableiten der kartenindividuellen Schlüssel SK.VSDD.AUT und SK.VSDD.ENC

Bezeichner	Typ	Gespeichert in	Nutzung für
SK.VSDD.AUT SK.VSDD.ENC	kartenindividuell symmetrisch	VSDD(*) eGK	Authentikation zwischen eGK und VSDD (inkl. Aushandlung Session-schlüssel)
KGK.VSDDCAMS.AUT KGK.VSDDCAMS.ENC	Masterschlüssel symmetrisch	CAMS und VSDD	Ableiten der kartenindividuellen Schlüssel SK.VSDDCAMS.AUT und SK.VSDDCAMS.ENC
SK.VSDDCAMS.AUT SK.VSDDCAMS.ENC	kartenindividuell symmetrisch	CAMS(*) und VSDD(*) eGK	Authentikation zwischen eGK und VSDD bzw. zwischen eGK und CAMS (inkl. Aushandlung Sessionschlüssel)
PrK.eGK.AUT	asymmetrisch	eGK	C2C-Authentikation eGK – HBA/SMC
PrK.CH.AUT	asymmetrisch	eGK	Elektronische Signatur
PrK.CH.AUTN	asymmetrisch	eGK	Elektronische Signatur
PrK.CH.ENC	asymmetrisch	eGK	Entschlüsseln
PrK.CH.ENCV	asymmetrisch	eGK	Entschlüsseln
PIN.CH	PIN	eGK	Benutzerauthentikation
PUK.CH	PIN	CAMS eGK	Rücksetzen FBZ der PIN.CH
PIN.home	PIN	eGK	Benutzerauthentikation
PUK.home	PIN	CAMS eGK	Rücksetzen FBZ der PIN.home
Geheimer herausgeber-spezifischer Zufallswert	Zufallswert (8 Byte)	CAMS	Berechnung des Pseudonyms für das AUTN-Zertifikat [gemX.509-pseu]

(*): Die kartenindividuellen Schlüssel müssen im CAMS bzw. VSDD nur dann gespeichert werden, falls diese zufällig erzeugt und nicht von einem Masterschlüssel abgeleitet werden.

Ggf. müssen zukünftig im Zusammenhang mit neuen Anwendungen weitere kryptographische Daten in einer eGK gespeichert werden.

Zusätzlich zu den in obiger Tabelle genannten geheimen kryptographischen Daten werden noch die folgenden weiteren "nicht-geheimen" (d.h. öffentlich verfügbaren) kryptographischen Daten in einer eGK gespeichert:

- CV-Zertifikat über den öffentlichen CV-Schlüssel der eGK,
- CA-CV-Zertifikat der CVC-CA, die das CV-Zertifikat der eGK erzeugt hat,

- öffentlicher Schlüssel der Root-CVC-CA, die das CA-CV-Zertifikat der CVC-CA erzeugt hat,
- X.509 Zertifikat über den öffentlichen AUT-Schlüssel des Kartenhinhabers,
- X.509 Zertifikat über den öffentlichen AUTN-Schlüssel des Karteninhabers (enthält ein Pseudonym anstelle des Namens),
- X.509 Zertifikat über den öffentlichen ENC-Schlüssel des Karteninhabers,
- X.509 Zertifikat über den öffentlichen ENCV-Schlüssel des Karteninhabers

Alle in der Tabelle genannten geheimen Schlüssel (außer den Masterschlüsseln KGK.CAMS.x, KGK.VSDD.x und KGK.VSDDCAMS.x), die PINs und PUKs sowie die aufgelisteten weiteren kryptographischen Daten müssen bei der Kartenproduktion in eine eGK eingebracht werden. Diese Daten können (mit Ausnahme der PINs) danach nicht mehr geändert werden.

Anmerkung zu privaten asymmetrischen Schlüsseln.

> Private Schlüssel für Signaturen, Authentisierung, Verschlüsselung (X.509) und auch die entsprechenden privaten CV-Schlüssel dürfen, wenn sie ihre Beweiskraft nicht verlieren wollen, nur einmal, nämlich in der Karte, existieren. Der Erzeuger und alle Überträger dieser privaten Schlüssel müssen über ihr Sicherheitskonzept nachweisen, dass sie diese privaten Schlüssel nicht gespeichert haben (siehe hierzu Abschnitt 4.1.2).

Anmerkung zum geheimen herausgeberspezifischen Zufallswert

> Der geheime herausgeberspezifische Zufallswert wird nicht in die eGK eingebracht. Er wird für die Generierung des Pseudonyms für das AUTN-Zertifikat benötigt (siehe hierzu [gemX.509-pseu]). Dieser Wert wird in diesem Dokument betrachtet, da er ggf. an den Personalisierer übertragen werden muss, falls dieser (bzw. eine durch ihn beauftragte X.509-CA) das Pseudonym im Rahmen der Zertifikatsgenerierung erzeugt.

Anmerkung zu den Masterschlüsseln KGK.CAMS.x, KGK.VSDD.x und KGK.VSDDCAMS.x

> Üblicherweise wird ein kartenindividueller symmetrischer Schlüssel von einem Masterschlüssel abgeleitet. Dieses Vorgehen ist aber keine feste Vorgabe. Es ist ebenso möglich, dass die kartenindividuellen Schlüssel einzeln generiert werden. In diesem Fall wird der zugehörige Masterschlüssel nicht benötigt.
>
> Sowohl ein Masterschlüssel wie auch Listen von kartenindividuellen Schlüsseln sind hochsensible Daten und entsprechend zu schützen. Jeder Zugriff auf den Masterschlüssel wie auch auf die Listen von kartenindividuellen Schlüsseln ist zu protokollieren.

Anmerkung zu den PINs (PIN.CH und PIN.home)

> Das genaue Vorgehen bezüglich des Eintragens von PINs während der Kartenproduktion ist noch nicht festgelegt. Zurzeit wird diskutiert, bei der Produktion einen konstanten Wert als Transport-PIN (im Sinne eine Null-PIN) in alle eGKs einzubringen. In diesem Fall entfällt die Notwendigkeit, einen PIN-Brief an den Karteninhaber zu senden.

Das Verfahren mit der konstanten Transport-PIN ist nicht mehr verwendbar, falls die zu produzierende eGK eine Folgekarte für den Karteninhaber ist und die Folgekarte direkt nach der Produktion bereits sensible Daten des Karteninhabers enthält oder mit der Folgekarte direkt ein Zugriff auf gespeicherte sensible Daten erlangt werden kann. In einem solchen Fall muss bei der Produktion eine geheime (Transport- oder Echt-) PIN in die eGK eingebracht werden. Diese muss dann dem Karteninhaber mit einem PIN-Brief mitgeteilt werden (Auslieferung eGK und PIN-Brief siehe 4.1.4).

Anmerkung zu den PUKs (PUK.CH und PUK.home)

> Bei einer PUK soll die Möglichkeit bestehen, dass diese nicht direkt nach der Kartenausgabe per PUK-Brief dem Karteninhaber mitgeteilt werden muss, sondern dass der PUK-Brief mit der PUK erst bei Bedarf auf Nachfrage des Karteninhabers bei seiner Krankenversicherung übermittelt wird. Dabei muss der Karteninhaber vor der Übermittlung der PUK ausreichend sicher identifiziert werden. Die PUKs der produzierten Karten müssen entweder unter der Verantwortung des Kostenträgers (gesichert) gespeichert werden, oder es muss ein Ableitungsverfahren verwendet werden, bei dem die PUK (anhand der ICCSN und ggf. weiterer Kartendaten) aus einem Masterschlüssel abgeleitet wird. Es muss ausgeschlossen werden, dass der Kartenherausgeber mit der von ihm abgeleiteten PUK eine PIN auf der Karte setzen kann.

3.2 Datenfluss bei der Kartenproduktion

Eine eGK wird durch die Krankenversicherung des Karteninhabers ausgegeben. An der Produktion einer eGK sind verschiedene Organisationen beteiligt. Die folgende Abbildung gibt einen Überblick über die möglichen beteiligten Organisationen:

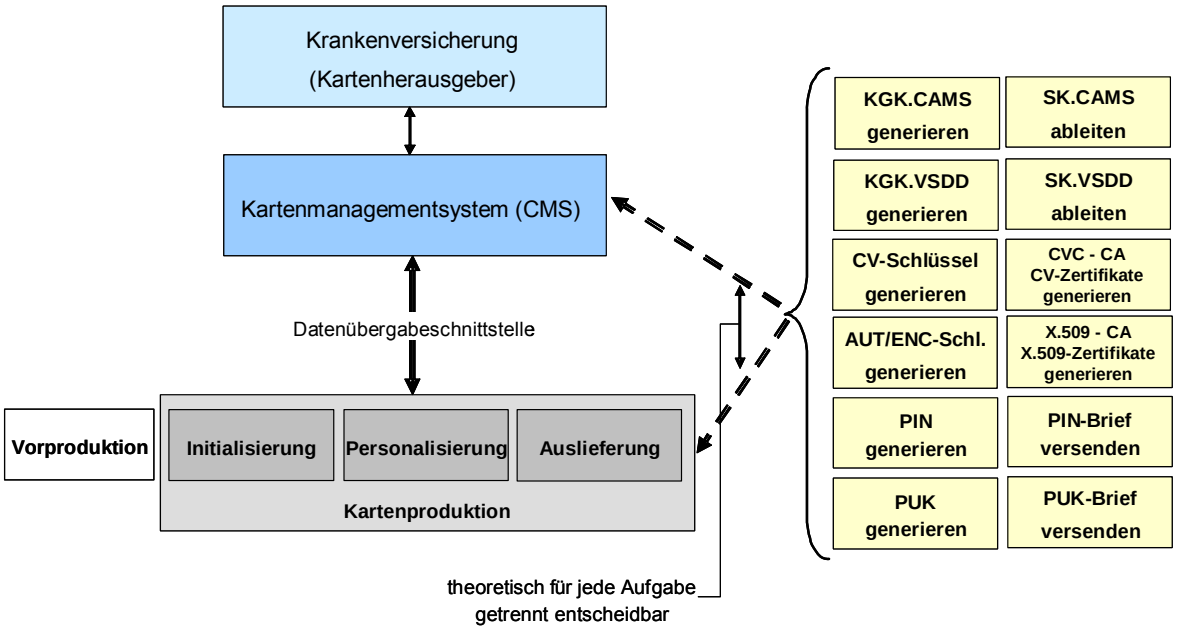

Abbildung 1 – Kartenproduktion: Beteiligte Organisationen/Rollen

Für das Zusammenspiel der Organisationen gibt es keine festen Vorgaben, diese müssen vielmehr bilateral zwischen den Beteiligten vereinbart werden. Der Datenfluss zwischen den einzelnen Organisationen muss ggf. verschlüsselt und integritätsgesichert sein. Die jeweilige Vereinbarung muss von der gematik zugelassen werden. In der Abbildung wird eine (logische) Organisation im Sinne einer Rolle betrachtet. Natürlich kann eine tatsächlich an der Kartenproduktion beteiligte Organisation mehrere der aufgezeigten Rollen übernehmen.

Die nicht-kryptographischen Daten werden für die Kartenproduktion durch das Kartenmanagementsystem des Kartenherausgebers bereitgestellt. Für die Übermittlung dieser Daten wird in [gemPers] eine XML-Schnittstelle definiert, die ab Version 1.1 auch den Austausch kryptographischer Daten ermöglicht.

Bezüglich der kryptographischen Daten werden in der Abbildung die einzelnen Aufgaben genannt, die im Rahmen einer Kartenproduktion ausgeführt werden müssen. Theoretisch können alle Aufgaben von unterschiedlichen Organisationen ausgeführt werden, in der Praxis werden aber einige Organisationen mehrere Aufgaben übernehmen. Die folgenden Anmerkungen müssen berücksichtigt werden, damit eine Organisation eine der genannten Aufgaben ausführen kann:

Anmerkung zu der Ableitung von SK.CAMS.x

> SK.CAMS.x ist ein kartenindividueller Schlüssel der eGK. Für die Ableitung wird ein Zugriff auf den Masterschlüssel KGK.CAMS.x sowie die ICCSN der eGK benötigt.
>
> Alternativ kann dieser Schlüssel kartenindividuell generiert werden.

Anmerkung zu der Ableitung von SK.VSDD.x

> SK.VSDD.x ist ein kartenindividueller Schlüssel der eGK. Für die Ableitung wird ein Zugriff auf den Masterschlüssel KGK.VSDD.x sowie die ICCSN der eGK benötigt.
>
> Alternativ kann dieser Schlüssel kartenindividuell generiert werden.

Anmerkung zum Generieren von KGK.VSDDCAMS.x und der Ableitung von SK.VSDDCAMS.x

> Es gelten die gleichen Anforderungen wie für das Generieren von KGK.CAMS.x und für das Ableiten von SK.CAMS.x.
>
> Generieren des Masterschlüssels und Ableitung der kartenindividuellen Schlüssel werden durch die gleichen Organisationen wie für KGK.CAMS.x und SK.CAMS.x übernommen.

Anmerkung zu der X.509 CA

> Es wird davon ausgegangen, dass die Zertifikate für die öffentlichen Schlüssel AUT, AUTN, ENC und ENCV von einer durch die gematik zugelassenen X.509-CA erzeugt und signiert werden. Der CA-Betreiber hat nachzuweisen, dass er nicht mehr Zertifikate signiert hat als dokumentiert.
>
> Die X.509-CA erzeugt X.509 Zertifikate über die öffentlichen AUT-, AUTN-, ENC- und ENCV-Schlüssel einer eGK. Diese Zertifikate sind personengebunden. Die X.509-CA benötigt für das Erzeugen der AUT-, ENC-

und ENCV-Zertifikate den Namen des späteren Karteninhabers sowie die öffentlichen Schlüssel. Siehe hierzu auch [gemX.509-eGK].

In das Zertifikat für den AUTN-Schlüssel wird anstelle des Namens des Karteninhabers ein Pseudonym eingestellt. In die Berechnung dieses Pseudonyms geht neben der KVNR ein herausgeberspezifischer geheimer Zufallswert ein. Die X.509-CA benötigt daher die KVNR des späteren Karteninhabers. Falls dieses Pseudonym nicht durch den Kartenherausgeber sondern durch die X.509-CA erzeugt wird, muss dieser Zufallswert der X.509-CA bekannt sein. Zum Aufbau der Pseudonyme siehe [gemX.509-pseu].

Die X.509-CA unterhält einen Sperrdienst für die von ihr ausgestellten Zertifikate. Da der Kartenherausgeber über sein Kartenmanagementsystem die Möglichkeit haben soll, die Sperrung eines Zertifikats zu veranlassen, benötigt das Kartenmanagementsystem mindestens einen sicheren authentischen Kanal zu dem Dienst der entsprechenden X.509-CA. Die Abläufe bei der Sperrung und Sperrgründe sind im Dokument [gemX.509-CP] festgelegt.

Anmerkung zu der CVC-CA

Die CVC-CA erzeugt und signiert ein CV-Zertifikat über den öffentlichen CV-Schlüssel einer eGK. Dieses Zertifikat ist kartenbezogen. Die CVC-CA benötigt daher für das Erzeugen dieses CV-Zertifikats die ICCSN der eGK sowie den öffentlichen CV-Schlüssel.

Der CA-Betreiber hat nachzuweisen, dass er nicht mehr Zertifikate signiert hat als dokumentiert.

Anmerkung zu dem Versenden von PIN- und PUK-Briefen

Für das Versenden eines PIN- bzw. PUK-Briefes wird ein Zugriff auf die PIN bzw. die PUK benötigt. Falls die PUK abgeleitet wird, wird ein Zugriff durch den Kartenherausgeber auf den Masterschlüssel und die Ableitungsdaten (z.B. die ICCSN) benötigt. In jedem Fall müssen PIN und PUK unter Einhaltung entsprechenden Sicherheitsanforderungen vom Erzeuger an den Versender übermittelt werden.

Unabhängig davon, welche Organisationen welche der bezüglich der kryptographischen Daten genannten Aufgaben übernehmen, müssen die entsprechenden Daten bei der Kartenproduktion zur Verfügung stehen. Für die Zuordnung der Aufgaben im Rahmen der Kartenproduktion sind dabei unter Verantwortung des Kartenherausgebers zwei unterschiedliche Vorgehensweisen möglich:

- Die Organisation, die eine Aufgabe übernimmt, erfüllt diese im Auftrage (bzw. als Teil) des Kartenherausgebers. Die erzeugten Daten werden von der Organisation an das CMS des Kartenherausgebers gegeben. Diese leitet die Daten über die erweiterte Datenübergabeschnittstelle an die Kartenproduktion weiter.

- Die Organisation, die eine Aufgabe übernimmt, erfüllt diese direkt im Auftrage (bzw. als Teil) der Kartenproduktion. Die erzeugten Daten werden von der Organisation direkt an die Kartenproduktion gegeben. Dieses leitet ggf. die Daten über die erweiterte Datenübergabeschnittstelle an das CMS des Kartenherausgebers weiter, falls dieses die Daten ebenfalls benötigt.

Für verschiedene Aufgaben kann die gewählte Zuordnung unterschiedlich sein. Die folgende Tabelle zeigt in Abhängigkeit von der Zuordnung einer Aufgabe zu dem

Kartenmanagement oder der Kartenproduktion, welche Daten über die Datenübergabeschnittstelle an die jeweils andere Seite übermittelt werden müssen:

Tabelle 2 – Verteilung der kryptographischen Daten

	Kartenmanagement → Kartenproduktion	Kartenproduktion → Kartenmanagement
KGK.CAMS.x generieren	KGK.CAMS.x, nur falls Kartenproduktion die Schlüssel SK.CAMS.x ableiten soll	KGK.CAMS.x
SK.CAMS.x ableiten/gener.	SK.CAMS.x	SK.CAMS.x, nur falls dieser karten-individuell generiert wird
KGK.VSDD.x generieren	KGK.CAMS.x nur falls Kartenproduktion die Schlüssel SK.CAMS ableiten soll.	KGK.VSDD.x
SK.VSDD.x ableiten	SK.VSDD.x	SK.VSDD.x, nur falls dieser karten-individuell generiert wird
KGK.VSDDCAMS.x generieren	KGK.VSDDCAMS.x, nur falls Kartenproduktion die Schlüssel SK.VSDDCAMS.x ableiten soll	KGK.VSDDCAMS.x
SK.VSDDCAMS.x ableiten/gener.	SK.VSDDCAMS.x	SK.VSDDCAMS.x, nur falls dieser kartenindividuell generiert wird
CV-Schlüssel generieren	CV-Schlüssel	-
CVC-CA	CV-Zertifikat	-
AUT/ENC-Schl. generieren	AUT/AUTN/ENC/ENCV-Schlüssel	-
X.509 CA	X.509-Zertifikate für AUT-, AUTN-, ENC- und ENCV-Schlüssel	Referenz auf die X.509-CA, um Zugriff auf den Sperrdienst zu haben
PIN generieren	PIN	PIN, falls Kartenmanagement den PIN Brief versendet
PIN Brief versenden	-	-
PUK generieren	PUK	PUK, falls Kartenmanagement den PUK Brief versendet
PUK Brief versenden	-	-

Anmerkung:

Private Schlüssel für Signaturen dürfen, wenn sie ihre Beweiskraft nicht verlieren wollen, nur einmal, nämlich in der Karte, existieren. Der Erzeuger und alle Übertrager eines privaten Schlüssels müssen beweisen, dass sie ihn nicht gespeichert haben (siehe hierzu Abschnitt 4.1.2).

4 Allgemeine Sicherheitsanforderungen

Die Sicherheit der kryptographischen Daten einer eGK ist für die Sicherheit der gesamten Telematikinfrastruktur eine notwendige Voraussetzung. Unabhängig von der Zuordnung der Aufgaben zu Organisationen und der Zusammenarbeit zwischen den an der Kartenproduktion beteiligten Organisationen müssen daher gewisse übergeordnete Sicherheitsanforderungen bezüglich des Umgangs mit den kryptographischen Daten erfüllt werden. Diese Sicherheitsanforderungen werden im Folgenden zusammengefasst.

Zertifizierungsinstanzen (CVC-CA, X.509-CA) einer PKI der Telematikinfrastruktur müssen bei ihrer Arbeit bezüglich der Sicherheit Mindestanforderungen erfüllen, die durch die gematik vorgegeben werden. Diese werden in [gemPKI-CVCGK], [gemPKI-Reg] und [gemTSL-SP_CP] beschrieben. Die im Folgenden angegebenen übergeordneten Sicherheitsanforderungen müssen für diese Zertifizierungsinstanzen im Sinne einer Konkretisierung der Mindestanforderungen in Bezug auf die Personalisierung einer eGK interpretiert werden. Ggf. in [gemPKI-CVCGK], [gemPKI-Reg] und [gemTSL-SP_CP] enthaltene höhere Sicherheitsanforderungen bleiben erhalten.

4.1 Vorgaben für das Mindestniveau

4.1.1 Schutzbedarfsfeststellung

Bezüglich des gesamten Prozesses der Produktion einer eGK wird der Schutzbedarf[1] sehr hoch vorgegeben für die Punkte

- Vertraulichkeit der geheimen kryptographischen Schlüssel,
- Vertraulichkeit der vorhandenen PINs und PUKs,

und hoch für die

- Authentizität der produzierten eGKs (siehe Abschnitt 4.1.4)

4.1.2 Sicherheit geheimer kryptographischer Schlüssel

Zu den geheimen kryptographischen Schlüsseln gehören alle symmetrischen Schlüssel (Masterschlüssel und kartenindividuelle Schlüssel) und die privaten Teile der asymmetrischen Schlüsselpaare.

Es gelten die folgenden Anforderungen:

- Ein geheimer Schlüssel (bei einem asymmetrischen Schlüssel das Schlüsselpaar) muss in einem dafür zugelassenen HSM[2] generiert werden.

[1] Schutzbedarf eingeteilt in niedrig, mittel, hoch und sehr hoch gemäß Schutzbedarfsanalyse des Sicherheitskonzepts der gematik

[2] Werden HSM-Module im Rahmen der Personalisierung eingesetzt, muss das Modul FIPS 140-2 Level 3, CC EAL4, ITSEC E3 oder einem äquivalenten Standard der Stärke „hoch“ genügen.

- Ein geheimer Schlüssel darf ein HSM nie in Klartext, sondern nur im Rahmen festgelegter Verfahren und verschlüsselt mit einem von der gematik zugelassenen Krypto-Verfahren verlassen.
- Für die Generierung eines geheimen Schlüssels müssen geeignete Verfahren verwendet werden, die dem aktuellen Stand der Technik und den Vorgaben des Sicherheitskonzepts der gematik entsprechen und ggf. vorhandenen zusätzlichen Anforderungen (z.B. BSI, Bundesnetzagentur) bezüglich des geforderten Sicherheitsniveaus genügen.
- Alle kryptographischen Berechnungen mit dem geheimen Schlüssel müssen innerhalb eines HSM erfolgen. Der Zugriff auf einen privaten Schlüssel in einem HSM muss durch eine Authentifikation geschützt sein. Die Zugriffe müssen protokolliert werden, das Zugriffssystem muss durch die gematik zugelassen sein.

Als HSM kann eine Chipkarte zum Einsatz kommen. Es wird dabei unterschieden zwischen

- einem Produktions-HSM, das durch eine beteiligte Organisation für die Absicherung kryptographischer Daten von der Generierung bis zum Einbringen in eine eGK verwendet wird, und
- der eigentlichen eGK, in die die kryptographischen Daten personalisiert werden.

Für die geheimen kryptographischen Schlüssel einer eGK gelten bezüglich ihrer Speicherung in einem Produktions-HSM noch die folgenden Vorgaben:

- Ein geheimer Schlüssel einer eGK darf in einem Produktions-HSM nur dann gespeichert werden, falls dies für die Produktion einer eGK direkt notwendig ist. Die Notwendigkeit muss im Sicherheitskozept begründet und im Sicherheitsgutachten bewertet werden.
- Ein geheimer Schlüssel einer eGK muss in einem Produktions-HSM aktiv gelöscht werden, sobald er durch dieses Produktions-HSM nicht mehr benötigt wird.

Analoge Vorgaben gelten für die (kryptographisch abgesicherte) Speicherung von geheimen Schlüsseln einer eGK außerhalb eines HSMs:

- Ein geheimer Schlüssel einer eGK darf außerhalb eines HSM nur dann (kryptographisch abgesichert) gespeichert werden, falls dies für die Produktion einer eGK direkt notwendig ist.
- Ein außerhalb eines HSM (kryptographisch abgesichert) gespeicherter geheimer Schlüssel einer eGK muss unverzüglich gelöscht werden, sobald dieser durch das speichernde System nicht mehr benötigt wird.

4.1.3 Sicherheit von PINs und PUKs

Eine eGK enthält (gemäß aktueller Spezifikation) eine PIN.CH und eine PIN.home sowie ggf. zugehörige PUKs. Bei einer PIN muss zwischen einer Transport- und einer Echt-PIN unterschieden werden. Bei einer Transport-PIN kann weiter zwischen einer geheimen kartenindividuellen Transport-PIN und einer allgemein bekannten konstanten Transport-PIN (z.B. Null-PIN Verfahren) unterschieden werden (Details siehe Dokument [gemeGK-PINPUK]).

Im Rahmen der Personalisierung einer eGK gelten für den Umgang mit geheimen Transport-PINs, Echt-PINs und PUKs die folgenden Anforderungen:

- Geheime Transport-PINs, Echt-PINs und PUKs müssen in einem zugelassenen HSM[3] generiert werden.
- Durch das Verfahren zum Generieren muss sichergestellt werden, dass PIN oder PUK zufällig und gleich verteilt über den gesamten zur Verfügung stehenden Zahlenraum erzeugt werden.
- Geheime Transport-PINs, Echt-PINs und PUKs dürfen ein HSM nie in Klartext verlassen. Ausnahme hiervon gilt nur für eine gesondert gesicherte Umgebung für den Druck eines PIN- bzw. PUK-Briefes.

Falls eine personalisierte eGK direkt sensible Daten des Karteninhaber enthält bzw. mit einer personalisierten eGK direkt Zugriff auf sensible Daten des Karteninhabers erhalten werden kann, gilt zusätzlich die folgende Forderung:

- Die eGK darf nicht mit einer allgemein bekannten konstanten Transport-PIN personalisiert werden.

Für geheime Transport-PINs, Echt-PINs und PUKs einer eGK gelten bezüglich ihrer Speicherung in einem Produktions-HSM noch die folgenden Vorgaben:

- Eine geheime Transport-PIN, Echt-PIN oder PUK einer eGK darf in einem Produktions-HSM nur dann gespeichert werden, falls dies für die Produktion einer eGK direkt notwendig ist.
- Eine geheime Transport-PIN, Echt-PIN oder PUK einer eGK muss in einem Produktions-HSM aktiv gelöscht werden, sobald er durch dieses Produktions-HSM nicht mehr benötigt wird.

Analoge Vorgaben gelten für die (kryptographisch abgesicherte) Speicherung von geheimen Transport-PINs, Echt-PINs und PUKs einer eGK außerhalb eines HSMs:

- Eine geheime Transport-PIN, Echt-PIN oder PUK einer eGK darf außerhalb eines HSM nur dann (kryptographisch abgesichert) gespeichert werden, falls dies notwendig und zugelassen ist.
- Ein außerhalb eines HSM (kryptographisch abgesichert) gespeicherte geheime Transport-PIN, Echt-PIN oder PUK einer eGK muss unverzüglich gelöscht werden, sobald diese durch das speichernde System nicht mehr benötigt wird.

[3] Werden HSM-Module im Rahmen der Personalisierung eingesetzt, muss das Modul FIPS 140-2 Level 3, CC EAL4, ITSEC E3 oder einem äquivalenten Standard der Stärke „hoch“ genügen

Falls eine PIN bzw. eine PUK durch Ableitung von einem Masterkey generiert wird, muss sichergestellt werden, dass diese Ableitung nur in hierfür im Sicherheitskonzept beschriebenen notwendigen Fällen geschieht.

Es muss sichergestellt werden, dass PIN und PUK in einem PIN-Brief immer nur an den korrekten Karteninhaber übermittelt werden.

Falls ein nachträglicher Abruf eines PUK-Briefes (im Bedarfsfalle) möglich sein soll, muss sichergestellt werden, dass der PUK-Brief nur durch hierfür autorisierte Personen abgerufen werden kann.

Anmerkung: Die genannten Anforderungen gelten für die Personalisierung einer eGK. Entsprechende Anforderungen an die Einsatzumgebung bezüglich des Umgangs mit PIN/PUK bzw. deren Verarbeitung bei der Nutzung einer eGK werden an anderer Stelle geklärt.

4.1.4 Authentizität einer eGK

Eine eGK muss einem konkreten Karteninhaber zugeordnet sein und bei der Personalisierung die zugehörigen korrekten (kryptographischen) Daten erhalten. Folgende Punkte müssen daher durch die korrekte Zusammenarbeit aller an der Personalisierung beteiligten Organisationen sichergestellt werden:

- Die beteiligen (CVC- und X.509-) CAs müssen entsprechend [gemPKI-Reg] und [gemTSL-Reg] als berechtigte CAs durch die gematik registriert und zugelassen sein.
- Eine eGK darf nur im Auftrage eines berechtigten Kartenherausgebers (eines Kostenträgers) personalisiert werden.
- Eine eGK muss eindeutig einem Karteninhaber (einer natürlichen Person) auf Basis der angelieferten Versichertendaten zugeordnet sein. Elektrisch und optisch personalisierte Daten müssen zu der gleichen Person gehören.
- Ein generierter Datensatz mit kartenindividuellen Schlüsseln darf nicht in zwei verschiedene eGKs eingebracht werden.
- Die in einer eGK enthaltenen X.509-Zertifikate für die AUT-, AUTN-, ENC- und ENCV- Schlüsselpaare müssen dem korrekten Karteninhaber (s.o.) zugeordnet sein.
- Das in einer eGK enthaltene CV-Zertifikat für das CV-Schlüsselpaar muss die korrekte ICCSN der eGK enthalten. Die eGK muss zusätzlich das korrekte CA-CV-Zertifikat der zugehörigen CVC-CA und den korrekten öffentlichen Schlüssel der Root-CVC-CA enthalten (diese CVC-Daten sind nach der Personalisierung nicht überschreib- bzw. löschbar).
- Falls die eGK bei der Personalisierung eine individuelle (Transport-) PIN erhält, muss der zugehörige PIN-Brief an den korrekten Karteninhaber übersendet werden.
- Falls die eGK bei der Personalisierung eine individuelle PUK erhält, muss der zugehörige PUK-Brief (sofort bzw. nur bei Bedarf zu einem späteren Zeitpunkt) an den korrekten Karteninhaber übersendet werden.

- Eine eGK, die vor Ausgabe an den Karteninhaber als fehlerhaft erkannt wird, muss ordnungsgemäß vernichtet werden.
- Eine eGK, die fehlerfrei produziert wurde, muss an den korrekten Karteninhaber übergeben werden.

4.1.5 Schlüssellängen, Algorithmen

Die durch eine eGK zu verwendenden Schlüssellängen und Algorithmen werden durch die gematik vorgegeben. Dabei werden Anforderungen Dritter (z.B. BSI) oder Verordnungen (z.B. von der BNA) durch die gematik berücksichtigt. Zurzeit gelten die Vorgaben aus [gemSpec eGK-P1] und [gemSpec eGK-P2].

Die gematik kann die Vorgaben für die Schlüssellänge und die Algorithmen aufgrund neuer Erkenntnisse (z.B. des BSI oder der BNA) bezüglich der Sicherheit bestimmter Schlüssellängen und Algorithmen ändern. Die gematik informiert alle beteiligten Organisationen über entsprechende Änderungen.

Falls Schlüssellängen und Algorithmen für die kryptographischen Schlüssel neu auszugebender eGKs geändert werden, müssen die Vorgaben für die kryptographischen Schlüssel in einem Produktions-HSM (zur Absicherung der Kommunikation zwischen Komponenten der beteiligten Organisationen) entsprechend angepasst werden. Schlüssellängen und Algorithmen für die letztgenannten Schlüssel müssen mindestens die Anforderungen erfüllen, die für die Schlüssel der eGK gelten.

Im Falle der Änderung der Vorgaben durch die gematik sind alle beteiligten Organisationen verpflichtet, die neuen Vorgaben nach einer Übergangsfrist umzusetzen. Nach Ablauf der Übergangsfrist dürfen nur noch die neuen Schlüssellängen und ggf. die neuen Algorithmen genutzt werden.

Die Übergangsfrist wird (nach Abstimmung mit den beteiligten Organisationen) durch die gematik vorgegeben.

4.1.6 Anforderungen an ein HSM

Für eine eGK gelten die folgenden Anforderungen:

- Es dürfen nur die Chipkartentypen als eGK verwendet werden, die durch die gematik zugelassen sind. Falls eine Ausstattung mit einer QES oder das Nachladen der QES vorgesehen sind, muss der Chipkartentyp zusätzlich gemäß SigG evaluiert und zertifiziert sein.

Für ein Produktions-HSM gelten die folgenden Anforderungen:

- Als HSM muss ein Modul (bzw. eine Chipkarte) eingesetzt werden, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. 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.

Folgende Funktionen eines Produktions-HSM dürfen nur nach einer Authentikation des aufrufenden Systems möglich sein:

- Generieren eines geheimen Schlüssels bzw. einer PIN oder PUK,
- (kryptographisch abgesicherter) Export eines geheimen Schlüssels bzw. einer PIN oder PUK,
- (kryptographisch abgesicherter) Import eines geheimen Schlüssels bzw. einer PIN oder PUK,
- Löschen eines geheimen Schlüssels bzw. einer PIN oder PUK (falls dies durch das HSM unterstützt wird),
- Sperren der Zugriffe auf einen geheimen Schlüssel bzw. einer PIN oder PUK (falls dies durch das HSM unterstützt wird)

Das genaue Vorgehen bei der Authentikation kann durch den Betreiber festgelegt werden. Sichergestellt werden muss dabei aber, dass das HSM nur nach erfolgter Authentikation genutzt werden kann.

Falls notwendig kann aus Gründen der Hochverfügbarkeit bzw. hoher Performanzanforderungen (Möglichkeit zur Lastverteilung) ein Produktions-HSM geklont werden, indem die relevanten geheimen Schlüssel aus dem HSM (kryptographisch abgesichert) exportiert werden und in ein weiteres HSM importiert werden. Dabei müssen die folgenden Punkte berücksichtigt werden:

- Falls das Klonen eines HSM technisch möglich ist, muss der Vorgang in dem Sicherheitskonzept der Organisation gesondert beschrieben und in dem Sicherheitsgutachten gesondert bewertet werden. Dabei müssen insbesondere die Maßnahmen für die Gewährleistung der Sicherheit der geheimen Schlüssel als auch die (technischen und/oder organisatorischen) Maßnahmen für die Verhinderung des unautorisierten Erstellens von Klonen beschrieben (Sicherheitskonzept) und bewertet (Sicherheitsgutachten) werden. Dabei muss der Schutz gegen die besonderen Bedrohungen gewährleistet sein, die sich bei diesem Verfahren ergeben.
- Das Klonen eines Produktions-HSM darf nur durch (mindestens) zwei Mitarbeiter (Vier-Augen-Prinzip) möglich sein.
- Das Klonen eines Produktions-HSM muss protokolliert werden.
- Zu jeder Zeit muss einfach nachvollziehbar sein, wie viele Klone eines Produktions-HSM existieren.

Wenn es während der Personalisierung notwendig wird, eine bereits gefertigte Karte noch einmal zu produzieren – d.h. zu klonen – z. B. aufgrund einer fehlerhaften optischen Personalisierung, muss dies unter kontrollierten Bedingungen (4-Augen-Prinzip und kontrollierte Vernichtung der ursprünglichen Karte) erfolgen. Außer in diesem Fall ist das Klonen einer eGK nicht zulässig.

4.1.7 Protokollierung

Alle an der Personalisierung einer eGK beteiligten Organisationen müssen die Arbeit ihrer Systeme revisionssicher protokollieren. Das genaue Ausmaß der notwendigen Protokollierung hängt dabei von den konkreten Aufgaben der Organisation im Rahmen der Personalisierung ab. Anhand der Protokollierung muss aber in jedem Fall nachvollzogen werden,

- welche kryptographischen Daten in welcher Stückzahl wann erzeugt bzw. verarbeitet wurden,
- in wessen Auftrag die kryptographischen Daten erzeugt bzw. verarbeitet wurden,
- an wen die erzeugten/verarbeiteten kryptographischen Daten weitergeleitet wurden,
- welche eGK wann produziert wurde,
- in wessen Auftrag eine eGK produziert wurde,
- welche fehlerfrei produzierte eGK wohin durch wen ausgeliefert wurde und
- welche fehlerhaft produzierte eGK wann durch wen vernichtet wurde.

Falls durch weitere Dokumente nicht anders gefordert muss die Protokollierung nicht für jede einzelne eGK erfolgen. Es reicht vielmehr eine Protokollierung pro Bestellung/ Produktionslauf. Um die „Abzweigung“ von Wafern, Chip-Gurten oder Kartenrohlingen zu verhindern, sind auch alle vor der eigentlichen Personalisierung liegenden Produktionsschritte geeignet zu überwachen. (Hinweis: Die Chips auf den Karten stellen genügend Information zur Verfügung, um ihren Weg bis zum Wafer zurückverfolgen zu können.

4.1.8 Betriebliche Anforderungen

Das die kryptographischen Daten verarbeitende Kernsystem (insbesondere das HSM) einer an der Personalisierung einer eGK beteiligten Organisation muss in einem geschützten Bereich der Betriebsstätte untergebracht sein. 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).
- Der Zugang zu diesem Bereich wird protokolliert.
- Alle Zugänge/Fenster sind in geeigneter Weise gegen Einbruch gesichert.
- Ist keine berechtigte Person anwesend, wird der Bereich alarmüberwacht.
- Besuchern ist der Zugang nur in Begleitung autorisierter Mitarbeiter und nur zu notwendigen, im Sicherheitskonzept beschriebenen Zwecken erlaubt.

Ein die kryptographischen Daten verarbeitendes System 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 der geheimen Schlüssel nicht verringert wird. Entsprechende Maßnahmen müssen in einem solchen Fall gesondert in dem Sicherheitskonzept beschrieben und in dem Sicherheitsgutachten bewertet werden.

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

Falls 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

mit einen technischen Authentifikations-/Autorisierungsverfahren entsprechender Stärke gegen Manipulationen und unautorisierte Nutzung geschützt werden.

Ist das Kernsystem in ein Netzwerk eingebunden, muss mit einen technischen Authentifikations-/Autorisierungsverfahren entsprechender Stärke sichergestellt werden, dass

- über das Netzwerk nicht unautorisiert auf das Kernsystem zugegriffen werden kann und dass
- keine Informationen des Kernsystems über das Netzwerk unautorisiert weitergegeben werden können.

4.2 Umsetzung der Sicherheitsanforderungen

Die Einhaltung aller in Abschnitt 4.1 genannten Sicherheitsanforderungen kann nur durch eine geordnete Zusammenarbeit aller an der Personalisierung beteiligten Organisationen erreicht werden. Dazu ist notwendig, dass jede beteiligte Organisation die für sie relevanten Anforderungen umsetzt.

CVC-CA und X.509-CA müssen die Umsetzung der von der gematik vorgegebenen Mindestanforderungen in einem Sicherheitskonzept dokumentieren. Die korrekte Umsetzung muss der Betreiber durch Vorlage eines Sicherheitsgutachtens nachweisen (siehe dazu [gemPKI-Reg] und [gemTSL-SP_CP]).

Für andere an der Personalisierung kryptographischer Daten beteiligte Organisationen (außer CVC-CA und X.509-CA) kann der Kartenherausgeber in seiner Verantwortung für den Gesamtprozess der Kartenausgabe vergleichbare Anforderungen an das Erstellen eines Sicherheitskonzepts und die Vorlage eines Sicherheitsgutachtens stellen. Für diesen Fall müssen Sicherheitskonzept und Sicherheitsgutachten die in den beiden folgenden Abschnitten enthaltenen Mindestanforderungen erfüllen.

4.2.1 Anforderungen an ein Sicherheitskonzept

Der Betreiber eines Systems, das an der Personalisierung kryptographischer Daten einer eGK beteiligt ist, 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,
- 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 4.1.1 auszugehen.

4.2.2 Sicherheitsgutachten

Falls verlangt 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 anerkannten Gutachter erstellt werden. Aktuell werden die durch das BSI akkreditierten Prüfstellen als solche angesehen (siehe http://www.bsi.de/zertifiz/zert/pruefst.htm). Ein bereits beim Betreiber vorhandenes Sicherheitsgutachten kann anerkannt werden, falls dieses für ein System des Betreibers mit vergleichbaren oder höheren Sicherheitsanforderungen erstellt wurde und die Verarbeitung der kryptographischen Daten einer eGK unter gleichen Bedingungen wie das begutachtete System betrieben wird.

5 Übergabeschnittstelle für kryptographische Daten

5.1 Übergabe kryptographischer Daten über die Personalisierungsschnittstelle /Auftragsdaten

[gemPers] enthält eine XML-Spezifikation für die Übergabe der eGK-Produktionsdaten von dem CMS (des Kartenherausgebers) an den Personalisierer der eGKs. Ab Version 1.1.1 ist diese Schnittstelle in der Lage, bidirektional kryptographische Daten auszutauschen.

Dieser Abschnitt beschreibt die Übergabe kryptographischer Daten mittels der Personalisierungsschnittstelle unter Gewährleistung der Vertraulichkeit geheimer kryptographischer Daten mit einem (symmetrischen) Transportschlüssel. Dabei sind verschiedene Möglichkeiten bezüglich der Gültigkeit eines Transportschlüssels möglich:

- Ein Transportschlüssel wird durch das CMS generiert und für die Verschlüsselung von kryptographischen Daten bei allen in einem Personalisierungsauftrag enthaltenen eGKs genutzt.
- Ein Transportschlüssel wird durch das CMS generiert und für die Verschlüsselung von kryptographischen Daten nur bei einer in einem Personalisierungsauftrag enthaltenen eGK genutzt.
- Es ist möglich, dass bei der Verschlüsselung der kryptographischen Daten einer einzelnen eGK verschiedene Transportschlüssel zum Einsatz kommen. Dies wird vor allem dann der Fall sein, falls der Transportschlüssel nicht durch das CMS generiert wird sondern direkt durch den Erzeugen der zu verschlüsselnden kryptographischen Daten.

Die Transportschlüssel selber werden mit dem öffentlichen (RSA-)Schlüssel des Personalisierers verschlüsselt. Siehe dazu die Anmerkungen in Kapitel 6.

Die folgende Abbildung zeigt die relevanten Elemente der XML-Schnittstelle aus [gemPers]:

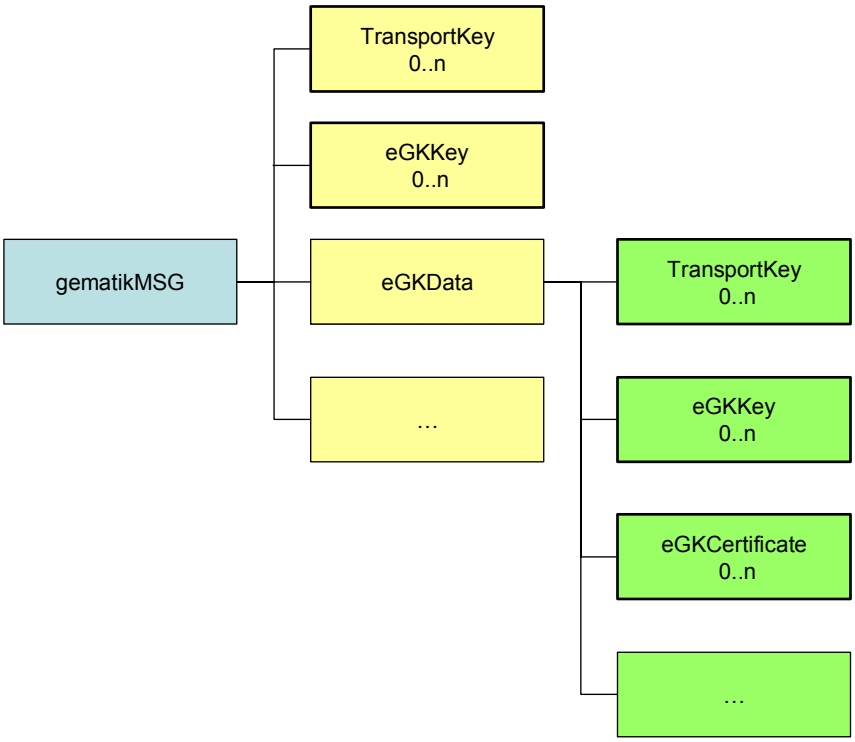

Abbildung 2 – Erweiterung der XML-Auftragsdaten

Der Aufbau der Elemente und ihr Einsatz werden in den folgenden Abschnitten beschrieben.

5.1.1 Element TransportKey

In einem Element `TransportKey` werden Daten für einen Transportschlüssel gespeichert. Es enthält ein Element `EncryptedKey` gemäß [XMLEnc] mit den folgenden Festlegungen:

- Das Element `EncryptedKey` enthält die Elemente `EncryptionMethod`, `ds:KeyInfo` und `CipherData`. Es besitzt das Attribut `ID='ref'`. Innerhalb eines Personalisierungsauftrages müssen alle enthaltenen Elemente `EncryptedKey` unterschiedliche Werte `ref` für das Attribut `ID` haben.
- Das Element `CipherData` enthält ein Element `CipherValue`, das wiederum den verschlüsselten Transportschlüssel enthält.
- Das Element `EncryptionMethod` ist leer, hat aber das Attribut `Algorithm='http://www.w3.org/2001/04/xmlenc#rsa-1_5'`.
- Das Element `ds:KeyInfo` enthält das Element `ds:KeyName`. Dieses enthält den Namen des Schlüssels, der für das Verschlüsseln des Transportschlüssels verwendet wurde.

Hinweis für das Verschlüsseln des Transportschlüssels:

Der Transportschlüssel ist ein 16 Byte langer Triple-DES Schlüssel. Diese 16 Byte werden mit dem öffentlichen Schlüssel des Empfängers der Daten unter Nutzung des Verschlüsselungsverfahren RSAES-PKCS1-v1_5-ENCRYPT aus [PKCS#1] verschlüsselt.

Anmerkung: Eine zukünftige Erweiterung um weitere Verschlüsselungsverfahren ist möglich.

Hinweis auf die Verwendung von Schlüsselnamen:

Der Transportschlüssel wird mit einem öffentlichen Schlüssel des Empfängers verschlüsselt. Der Empfänger kann dabei mehrere Schlüsselpaare haben. Unterschieden werden diese durch Schlüsselnamen, die der Empfänger den Schlüsselpaaren zuordnet. Der Versender stellt den Namen des tatsächlich verwendeten öffentlichen Schlüssels in das Element `ds:KeyName` ein. Siehe dazu auch Kapitel 6.

Hinweis zur Positionierung eines Elements `TransportKey`:

Falls der (verschlüsselt) enthaltene Transportschlüssel für die Verschlüsselung von kryptographischen Daten für mehrere im Personalisierungsauftrag enthaltenen eGKs verwendet wurde, muss das Element `TransportKey` als direktes Tochterelement von `gematikMSG` in der Datei enthalten sein. Wurden dagegen mit dem Transportschlüssel nur Daten für jeweils eine eGK verschlüsselt, muss das Element `TransportKey` als direktes Tochterelement von dem zu dieser eGK gehörenden Element `eGKData` in der Datei enthalten sein.

5.1.2 Element eGKCertificate

In einem Element `eGKCertificate` werden Daten für ein Zertifikat einer eGK gespeichert. Es besteht aus den beiden Unterelementen

- `CertificateSem`
- `CertificateValue`

Das Element `CertificateSem` enthält einen Namen (String), der das in `CertificateValue` enthaltene Zertifikat identifiziert. Aktuell können die folgenden Namen enthalten sein:

- CVC_CA_eGK.CS
- CVC.eGK.AUT
- C.CH.ENC
- C.CH.AUT
- C.CH.ENCV
- C.CH.AUTN

Das Element `CertificateValue` enthält das eigentliche Zertifikat. Die Daten müssen vor dem Einstellen gemäß Abschnitt 5.3.3 aufbereitet werden.

5.1.3 Element eGKKey

In einem Element `eGKKey` werden Daten für einen Schlüssel oder eine PIN bzw. PUK der eGK gespeichert. Es besteht aus den beiden Unterelementen

- `KeySem`
- `KeyValue`

Das Element `KeySem` enthält einen Namen (String), der den in `KeyValue` enthaltenen Wert (Schlüssel, PIN/PUK bzw. herausgeberspezifischer geheimer Zufallswert für die Pseudonymgenerierung) identifiziert. Aktuell können die folgenden Namen enthalten sein:

- PSEUDO.RND
- KGK.CAMS.AUT
- KGK.CAMS.ENC
- SK.CAMS.AUT
- SK.CAMS.ENC
- KGK.VSDD.AUT
- KGK.VSDD.ENC
- SK.VSDD.AUT
- SK.VSDD.ENC
- KGK.VSDDCAMS.AUT
- KGK.VSDDCAMS.ENC
- SK.VSDDCAMS.AUT
- SK.VSDDCAMS.ENC
- CV.eGK.Public
- CV.eGK.Private
- CV.Root.Public
- AUT.Public
- AUT.Private
- ENC.Public
- ENC.Private
- AUTN.Public

- AUTN.Private
- ENCV.Public
- ENCV.Private
- PIN.HOME
- PUK.HOME
- PIN.CH
- PUK.CH

Falls das Element `KeySem` einen der Werte PSEUDO.RND, KGK.CAMS.x, KGK.VSDD.x oder KGK.VSDDCAMS.x enthält, existiert das übergeordnete Element `eGKKey` nur einmal in dem Personalisierungsauftrag. Es ist dann Teil der Rahmendaten zum Auftrag. In allen anderen Fällen kann das übergeordnete Element `eGKKey` pro eGK im Personalisierungsauftrag vorkommen.

Das Element `KeyValue` enthält ein Element `EncryptedData` gemäß [XMLEnc] mit den folgenden Festlegungen:

- Das Element `EncryptedData` enthält die Elemente `EncryptionMethod`, `ds:KeyInfo` und `CipherData`.
- Das Element `CipherData` enthält das Element `CipherValue`, das wiederum die verschlüsselten Schlüsseldaten enthält. Die Daten müssen vor dem Einstellen gemäß den Abschnitten 5.3.1, 5.3.2 oder 5.3.4 aufbereitet werden.
- Das Element `EncryptionMethod` ist leer, hat aber das Attribut `Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-cbc'`.
- Das Element `ds:KeyInfo` enthält das Element `ds:RetrivalMethod`. Dieses ist selber leer, hat aber die beiden Attribute `URI='#ref'` und `Type='http://www.w3.org/2001/04/xmlenc#EncryptedKey'`. Die Referenz `ref` muss dabei den Wert des Attributes `ID` des Elements `EncryptedKey` haben, das den zugehörigen verschlüsselten Transportschlüssel enthält. Siehe hierzu 5.1.1.

5.2 Übergabe kryptographischer Daten über die Personalisierungsschnittstelle /Rückmeldedaten

Neben der Spezifikation der Schnittstelle für die Übergabe der eGK-Produktionsdaten von dem CMS (des Kartenherausgebers) an den Personalisierer der eGKs ist in [gemPers] auch die Schnittstelle für Rückmeldungen spezifiziert. Abhängig von dem genauen Zusammenspiel zwischen dem CMS und dem Personalisierer besteht die Notwendigkeit, kryptographische Daten einer produzierten eGK von dem Personalisierer an das CMS rückgemeldet werden.

Die Vertraulichkeit geheimer kryptographischer Daten wird durch eine Verschlüsselung mit einem (symmetrischen) Transportschlüssel gewährleistet. Dabei sind verschiedene Möglichkeiten bezüglich der Gültigkeit eines Transportschlüssels innerhalb einer Rückmeldung möglich:

- Ein Transportschlüssel wird durch den Personalisierer generiert und für die Verschlüsselung von kryptographischen Daten bei allen in einer Rückmeldung enthaltenen eGKs genutzt.
- Ein Transportschlüssel wird durch den Personalisierer generiert und für die Verschlüsselung von kryptographischen Daten nur bei einer in einer Rückmeldung enthaltenen eGK genutzt.

Die Transportschlüssel selber werden mit dem öffentlichen (RSA-)Schlüssel des CMS verschlüsselt. Siehe dazu die Anmerkungen in Kapitel 6.

Die folgende Abbildung zeigt die entsprechenden Elemente der Rückmelde-Schnittstelle aus [gemPers]:

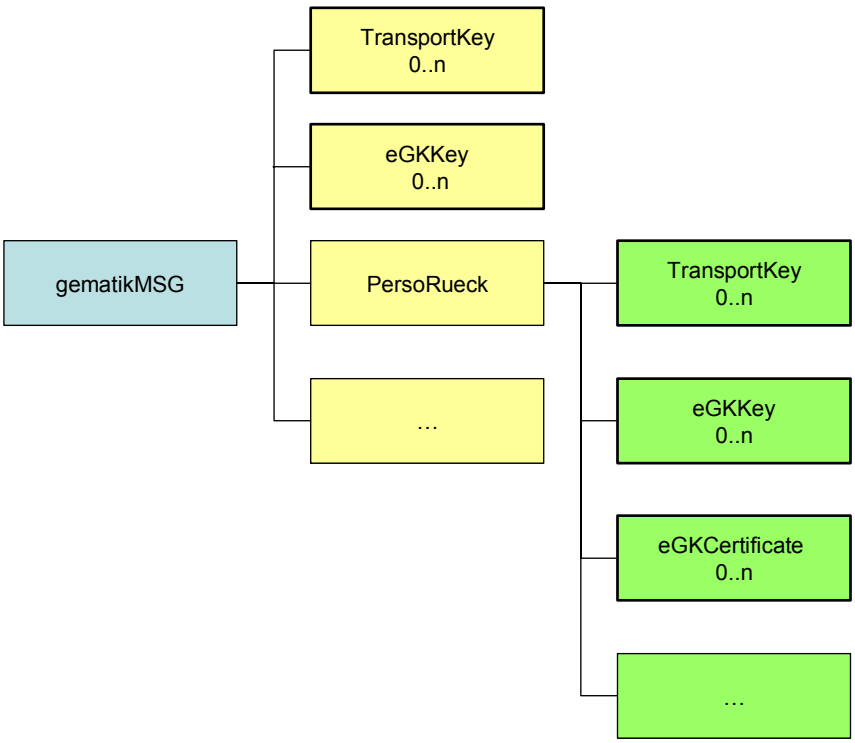

Abbildung 3 – Erweiterung der XML-Rückmeldedaten

Der genaue Aufbau der Elemente und ihr Einsatz werden in den Unterabschnitten von Abschnitt 5.1 beschrieben.

5.3 Aufbereitung der kryptographischen Daten für die Übertragung

Kryptographische Daten einer eGK werden bei der Übertragung in ein Element `CertValue` (Zertifikate) bzw. `KeyValue` (Schlüssel, PINs, PUKs) eingestellt. In den folgenden Abschnitten wird beschrieben, welche Bytes genau für die verschiedenen Daten in diese Elemente eingestellt werden müssen.

Schlüssel, PINs und PUKs werden bei der Übertragung mit einem Transportschlüssel T MAC-gesichert und verschlüsselt. Für Verschlüsselung und MAC-Sicherung werden die folgenden Bezeichnungen verwendet:

- ENC-T (a, B): Verschlüsselung von B mit dem Transportschlüssel T. Verwendet wird Triple-DES im CBC-Modus mit ICV a und Padding '80 00 … 00', wobei in jedem Fall mindestens ein Padding-Byte verwendet wird.
- MAC-T (a, B): Retail MAC über B mit dem Transportschlüssel T. Verwendet wird Triple-DES mit ICV a und Padding '80 00 … 00', wobei in jedem Fall mindestens ein Padding-Byte verwendet wird.

5.3.1 Symmetrische Schlüssel

Symmetrische Schlüssel einer eGK sind 16 Byte lange Triple-DES-Schlüssel. Ein solcher symmetrischer Schlüssel K wird mit einem Transportschlüssel T wie folgt verschlüsselt und MAC gesichert:

M = MAC-T (0, K)

Kryptogramm = ENC-T (0, '80 10 K 8E 08 M')

Der ICV 0 besteht dabei aus 8 Bytes '00'.

In das Element `KeyValue` werden dann (innerhalb von `CipherValue`) folgende Bytes base64 kodiert eingestellt:

'00 00 00 00 00 00 00 00' | Kryptogramm

5.3.2 Asymmetrische Schlüsselpaare

Asymmetrische Schlüsselpaare einer eGK sind RSA-Schlüsselpaare. Privater und öffentlicher Schlüssel werden getrennt in zwei Elementen `KeyValue` übertragen.

Die Komponenten eines privaten Schlüssels werden in folgender Struktur übertragen:

Tabelle 3 – TLV-Struktur für einen privaten Schlüssel

Tag	Length	Value
'7F 48'	'XX … XX'	
'92'	'XX … XX'	Parameter p
'93'	'XX … XX'	Parameter q

Tag	Length	Value
'94'	'XX … XX'	Parameter 1/q mod p
'95'	'XX … XX'	Parameter d mod (p – 1)
'96'	'XX … XX'	Parameter d mod (q – 1)
'81'	'XX … XX'	Modulus
'83'	'XX … XX'	Privater Exponent

Die Komponenten eines öffentlichen Schlüssels werden in folgender Struktur übertragen:

Tabelle 4 – TLV-Struktur für einen öffentlichen Schlüssel

Tag	Length	Value
'7F 49'	'XX … XX'	
'81'	'XX … XX'	Modulus
'82'	'XX … XX'	Öffentlicher Exponent

Die Längenfelder können dabei ein ('xx'), zwei ('81 xx') oder drei ('82 xx xx') Byte lang sein.

Sei S eine entsprechende Struktur für einen öffentlichen bzw. privaten Schlüssel. Eine solche Struktur wird mit einem Transportschlüssel T wie folgt verschlüsselt und MAC gesichert:

M = MAC-T (0, S)

Kryptogramm = ENC-T (0, 'B2 82 xx xx S 8E 08 M')

Mit '82 xx xx' muss dabei die Gesamtlänge der Struktur S kodiert werden.

Der ICV 0 besteht dabei aus 8 Bytes '00'.

In das Element `KeyValue` werden dann (innerhalb von `CipherValue`) folgende Bytes base64-kodiert eingestellt:

'00 00 00 00 00 00 00 00' | Kryptogramm

5.3.3 Zertifikate

Zertifikate werden bei der Übertragung nicht weiter kryptographisch abgesichert. In das jeweilige XML-Element `CertValue` wird der gesamte Inhalt der jeweiligen eGK-Datei base64-kodiert eingestellt.

Für ein CV-Zertifikat gilt dabei:

> Es werden alle Bytes gemäß den Tabellen B.12 und B.13 aus [gemSpec eGK-P1] beginnend mit dem Tag '7F21' und endend mit den 8 Byte CAR base64-kodiert eingestellt.

Für ein X.509-Zertifikat gilt dabei:

Das Zertifikat wird ohne weitere sonstige Bytes base64-kodiert eingestellt.

5.3.4 PINs und PUKs

PINs und PUKs einer eGK werden gemäß [gemSpec eGK-P1] in einem Format 2 PIN Block kodiert.

Ein solcher PIN Block B wird mit einem Transportschlüssel T wie folgt verschlüsselt und MAC gesichert:

M = MAC-T (0, B)

Kryptogramm = ENC-T (0, '80 08 B 8E 08 M')

Der ICV 0 besteht dabei aus 8 Bytes '00'.

In das Element `KeyValue` werden dann (innerhalb von `CipherValue`) folgende Bytes base64-kodiert eingestellt:

'00 00 00 00 00 00 00 00' | Kryptogramm

5.3.5 Herausgeberspezifischer geheimer Zufallswert

Dieser geheime Zufallswert RND ist 8 Byte lang. Er wird für die Ableitung der Pseudonyme benötigt (siehe [gemX.509-pseu]).

Ein solcher geheimer Zufallswert RND wird mit einem Transportschlüssel T wie folgt verschlüsselt und MAC gesichert:

M = MAC-T (0, RND)

Kryptogramm = ENC-T (0, '80 08 RND 8E 08 M')

Der ICV 0 besteht dabei aus 8 Bytes '00'.

In das Element `KeyValue` werden dann (innerhalb von `CipherValue`) folgende Bytes base64 kodiert eingestellt:

'00 00 00 00 00 00 00 00' | Kryptogramm

6 Vorgehen bei der Datenaufbereitung

6.1 Key-Management für die Transportschlüssel

Um die im letzten Kapitel eingeführte Erweiterung der Datenübergabeschnittstelle für die Übertragung kryptographischer Daten einer eGK korrekt nutzen zu können, werden zwei neue "Typen" von kryptographischen Schlüsseln benötigt:

- Transportschlüssel: Dies ist ein 16 Byte langer (symmetrischer) Triple-DES-Schlüssel. Er wird für das Ver- und Entschlüsseln der eigentlichen eGK-Daten verwendet.
- Key-Encryption-Key (KEK): Dies ist ein (asymmetrisches) RSA-Schlüsselpaar. Der zugehörige öffentliche Schlüssel wird zum Verschlüsseln eines Transportschlüssels verwendet, der zugehörige private Schlüssel wird entsprechend zum Entschlüsseln des Transportschlüssels verwendet.

Der KEK ist gemäß den Vorgaben aus dem Kryptographiekonzept des Sicherheitskonzepts sicher zu erzeugen und sicher aufzubewahren.

Für den Umgang mit diesen Schlüsseln gelten die gleichen Anforderungen aus Abschnitt 4.1 wie für die kryptographischen Daten einer eGK.

Für die Schlüssellänge gilt dabei folgende Konkretisierung:

- Ein KEK muss eine Mindestlänge von 2048 Bit haben.

Ein Transportschlüssel wird immer durch den Absender der mit ihm verschlüsselten Daten generiert. Die Gültigkeit des Transportschlüssels ist dabei maximal eine Nachricht (z.B. ein Personalisierungsauftrag). Ob für die Verschlüsselung der in einer Nachricht enthaltenen Daten ein oder mehrere Transportschlüssel zum Einsatz kommen, muss bilateral zwischen dem Absender und dem Empfänger geregelt werden.

Jedes CMS (bzw. jeder Kartenherausgeber) sowie jeder Personalisierer benötigt mindestens einen KEK. Für diesen gilt:

- Ein KEK wird durch seinen "Besitzer" selber generiert.
- Die Gültigkeit eines KEK beträgt maximal ein Jahr.
- Jedem KEK wird durch seinen Besitzer ein Schlüsselname zugeordnet. Anhand dieses Namens muss der Besitzer den KEK eindeutig bestimmen können. Ein Schlüsselname besteht dabei aus maximal 20 Zeichen.
- Will ein Kartenherausgeber eGKs mit einem Personalisierer bei der Produktion seiner eGKs zusammenarbeiten, müssen diese die öffentlichen Schlüssel und Schlüsselnamen ihrer KEKs austauschen. Dabei muss die Authentizität der ausgetauschten Schlüssel gewährleistet sein. Das genaue Vorgehen hierbei muss bilateral zwischen den Beteiligten abgestimmt werden. Die gematik lässt den verantwortlichen Kartenproduzenten zu und prüft das Verfahren.

Abhängig von dem gewählten Modell für die Zusammenarbeit der beteiligten Organisationen (siehe Abschnitt 6.2) kann es notwendig sein, dass auch ein Zulieferer von kryptographischen Daten den öffentlichen Schlüssel des Personalisierers erhält (siehe Variante in Abschnitt 6.2.2). In diesem Fall muss das CMS den vom Personalisierer erhaltenen öffentlichen Schlüssel (inkl. Schlüsselnamen) an die vom Kartenherausgeber beauftragten Zulieferer übermitteln. Dabei muss wieder die Authentizität des öffentlichen Schlüssels gewährleistet sein.

6.2 Modelle für die Zusammenarbeit

Wie in Abschnitt 3.2 dargestellt können verschiedene kryptographische Daten einer eGK von unterschiedlichen Organisationen (Erzeuger/Zulieferer) erzeugt werden. Für den Transport eines kryptographischen Datums von seiner Erzeugung bis in die eGK sind prinzipiell zwei unterschiedliche Alternativen denkbar:

- Die kryptographischen Daten einer eGK werden durch das CMS von den einzelnen Erzeugern bezogen (bzw. selber erzeugt). Danach stellt das CMS die Daten in einem Personalisierungsauftrag zusammen und sendet diesen an den Personalisierer. Es muss schlüssig nachgewiesen werden können, dass das CMS und alle am Prozess beteiligten Partner nach Abschluss der Kartenproduktion die privaten Schlüssel nach Einbringen in die eGK nicht mehr gespeichert haben.
- Die kryptographischen Daten einer eGK werden durch den Personalisierer von den einzelnen Erzeugern bezogen (bzw. selber erzeugt). Bei Bedarf werden diese Daten (teilweise) nach der Personalisierung in eine Rückmeldung auf den Personalisierungsauftrag zusammengestellt und an das CMS gesendet. Es muss schlüssig nachgewiesen werden können, dass das CMS und alle am Prozess beteiligten Partner nach Abschluss der Kartenproduktion die privaten Schlüssel nach Einbringen in die eGK nicht mehr gespeichert haben.

Bei der ersten Alternative hat der Kartenherausgeber die größere Kontrolle über die an der Produktion seiner eGKs beteiligten Zulieferer. Falls gewünscht (und technisch möglich) kann der Kartenherausgeber die kryptographischen Daten (bzw. Teile dieser) auch selber erzeugen. Der Personalisierer übernimmt bei dieser Alternative nur die reine Personalisierung der bei ihm durch den Kartenherausgeber bestellten eGKs.

Für die erste Alternative können zwei Varianten weiter unterschieden werden. Bei der ersten Variante verschlüsselt ein Zulieferer die Daten so, dass das CMS diese entschlüsseln kann (siehe Abschnitt 6.2.1), während er die Daten bei der zweiten Variante so verschlüsselt, dass nur der Personalisierer diese entschlüsseln kann (siehe Abschnitt 6.2.2).

Bei der zweiten Alternative (siehe Abschnitt 6.2.3) hat der Personalisierer die Aufgabe eines Generalunternehmers, wobei die Verantwortung bei dem Kartenherausgeber bleibt. Er entscheidet (in Abstimmung mit dem Kartenherausgeber), welche Zulieferer er für die kryptographischen Daten nutzt bzw. welche kryptographischen Daten er selber erzeugt. Der Kartenherausgeber bestellt eine bestimmte Anzahl eGKs bei dem Personalisierer. Er liefert aber nur die versicherungsfachlichen Daten für die bestellten eGKs.

In den folgenden Abschnitten werden die einzelnen Varianten mit ihren Vor- und Nachteilen näher beschrieben. Bei der Produktion von eGKs können die Varianten auch gemischt werden. Dabei kann eine Teilmenge der kryptographischen Daten durch das CMS selber (bzw. in dessen Auftrag) erzeugt werden, während der Rest der kryptographischen Daten durch den Personalisierer (bzw. in dessen Auftrag) erzeugt werden. Die in Kapitel 5 beschriebene Erweiterung der Übergabeschnittstelle zwischen einem CMS und einem Personalisierer kann für alle genannten Varianten und für mögliche Mischformen genutzt werden. Die in den folgenden Abschnitten aufgeführten Vor- und Nachteile der Varianten gelten aber nur noch eingeschränkt, falls Mischformen zum Einsatz kommen.

Unabhängig von dem gewählten Modell der Zusammenarbeit muss bei der konkreten Nutzung der Schnittstelle folgender Grundsatz berücksichtigt werden;

> Es dürfen nur solche kryptographischen Daten über die Schnittstelle zwischen CMS und Personalisierer ausgetauscht werden, die durch den Empfänger auch tatsächlich für seine Aufgaben benötigt werden. Die Aufgaben und die hierfür benötigten kryptographischen Daten müssen in dem Sicherheitskonzept beschrieben und begründet werden.

6.2.1 Zentrale Datenaufbereitung durch CMS

Bei dieser Variante entscheidet der Kartenherausgeber zunächst, welche kryptographischen Daten er in seinem CMS selber erzeugen will und welche er von Zulieferern beziehen möchte. Ggf. wählt er die entsprechenden Zulieferer aus.

Die Schnittstelle zwischen dem CMS und den Zulieferern muss zwischen diesen bilateral festgelegt werden. Dabei müssen bezüglich der Sicherheit der übertragenen kryptographischen Daten die Anforderungen aus Kapitel 3 erfüllt werden. Als Grundlage für diese Schnittstelle können die Vorgaben aus Abschnitt 5.1 verwendet werden.

Vor der Übertragung von kryptographischen Daten von einem Zulieferer an ein CMS muss der öffentliche Schlüssel und der Schlüsselname des KEK des CMS an den Zulieferer übermittelt werden. Dabei muss die Authentizität des KEK gewährleistet werden. Siehe dazu auch die Ausführungen in Abschnitt 6.1.

Für einen Zulieferer gilt:

> Der Zulieferer muss die kryptographischen Daten generieren und für die Übertragung aufbereiten. Bei der Übertragung müssen ggf. einige der Daten mit einem Transportschlüssel MAC-gesichert und verschlüsselt werden. Dieser Transportschlüssel wird durch den Zulieferer generiert. Der Transportschlüssel wiederum muss mit dem öffentlichen Schlüssel des KEK des CMS verschlüsselt werden. Das genaue Vorgehen bei der Aufbereitung der Daten muss zwischen dem Kartenherausgeber und dem Zulieferer bilateral abgestimmt werden. Es können die Vorgaben aus Abschnitt 5.3 genutzt werden.

Für das CMS gilt:

> Das CMS muss die von einem Zulieferer enthaltenen verschlüsselten Daten entschlüsseln. Dazu müssen zunächst die verwendeten Transportschlüssel mit dem privaten Schlüssel des eigenen KEK entschlüsselt werden.

Das CMS generiert die für einen Personalisierungsauftrag benötigten Transportschlüssel. Dabei gibt es prinzipiell die beiden folgenden Möglichkeiten:

- Es wird nur ein Transportschlüssel für den ganzen Personalisierungsauftrag generiert. Dieser wird für das ggf. notwendige Verschlüsseln (und die zugehörige MAC-Sicherung) aller in dem Auftrag enthaltenen kryptographischen Daten aller enthaltenen eGKs eingesetzt. In diesem Fall enthält in dem Personalisierungsauftrag nur das Element `gematikMSG` ein Tochterelement `TransportKey`, das den verschlüsselten Transportschlüssel enthält.

- Es wird ein Transportschlüssel pro in dem Auftrag enthaltener eGK generiert. Ein Transportschlüssel wird dann nur für das ggf. notwendige Verschlüsseln (und die zugehörige MAC-Sicherung) der kryptographischen Daten einer in dem Auftrag enthaltenen eGK eingesetzt. Dies ist das empfohlene Vorgehen. In diesem Fall enthält in dem Personalisierungsauftrag jedes enthaltene Element `eGKData` ein Tochterelement `TransportKey`, das den verschlüsselten Transportschlüssel enthält.

  In jedem Fall wird ein Transportschlüssel mit dem öffentlichen Schlüssel des KEK des Personalisierers verschlüsselt und in ein Element `TransportKey` in den Personalisierungsauftrag eingestellt. Das Vorgehen dabei und der genaue Aufbau des Elements `TransportKey` sind in Abschnitt 5.1.1 beschrieben.

  Die kryptographischen Daten einer eGK müssen durch das CMS gemäß den Vorgaben aus Abschnitt 5.3 aufbereitet werden und in ein Element `eGKCertificate` (Aufbau gemäß Abschnitt 5.1.2) bzw. `eGKKey` (Aufbau gemäß Abschnitt 5.1.3) in den Personalisierungsauftrag eingestellt werden.

Für den Personalisierer gilt:

Der Personalisierer erhält einen Auftrag mit der XML-Struktur gemäß Abschnitt 5.1.

Alle in einem Element `TransportKey` enthaltenen Transportschlüssel müssen mit dem privaten Schlüssel des eigenen KEK entschlüsselt werden. Um den richtigen KEK zu bestimmen muss ggf. der (in dem zugehörigen Element `ds:KeyName` enthaltene) Schlüsselname ausgewertet werden.

Alle in einem Element `eGKKey` enthaltenen verschlüsselten Daten müssen mit dem korrekten Transportschlüssel entschlüsselt werden. Danach muss der MAC überprüft werden. Der korrekte Transportschlüssel wird über die Referenz in dem Attribut `URI` des zugehörigen Elements `ds:RetrivalMethod` bestimmt.

Nach dem Entschlüsseln eines kryptographischen Datums mit dem Transportschlüssel muss dieses ggf. (abhängig vom konkreten Kartenbetriebssystem) mit einem kartenindividuellen Personalisierungsschlüssel verschlüsselt (und ggf. MAC-gesichert) werden. Das genaue Vorgehen hierbei ist abhängig von dem konkreten Kartenbetriebssystem.

Nach der Personalisierung werden keine kryptographischen Daten über die Rückmeldung an das CMS zurückgegeben.

Vorteile dieser Variante sind:

- Der Kartenherausgeber kann frei entscheiden, ob (bzw. welche) kryptographische Daten selber erzeugt werden bzw. von einem Zulieferer bezogen werden.
- Der Kartenherausgeber hat die volle Kontrolle über die Zusammenstellung aller Daten eines Personalisierungsauftrags.
- Die Entscheidung, welcher Personalisierer beauftragt werden soll, kann auch nach der Bestellung kryptographischer Daten bei einem Zulieferer (bzw. auch nach deren Lieferung) gefällt werden.
- Alle zu einer eGK gehörenden kryptographischen Daten können mit dem gleichen Transportschlüssel verschlüsselt werden.
- Der öffentliche Schlüssel des Personalisierers muss nur an den CMS übermittelt werden.. Er muss nicht an die einzelnen Zulieferer weitergeleitet werden.

Nachteile dieser Variante sind:

- Alle von einem Zulieferer verschlüsselt erhaltenen kryptographischen Daten müssen durch das CMS entschlüsselt und wieder verschlüsselt werden.
- Theoretisch besteht die Möglichkeit, dass das CMS Kenntnis über die von einem Zulieferer erhaltenen kryptographischen Daten erlangen. Deshalb muss schlüssig nachgewiesen werden können, dass das CMS und alle am Prozess beteiligten Partner nach Abschluss der Kartenproduktion die privaten Schlüssel nach Einbringen in die eGK nicht mehr gespeichert haben.

6.2.2 Datenzusammenführung durch CMS

Diese Variante ist ähnlich zu der in Abschnitt 6.2.1 beschriebenen Variante. Abweichend zu Abschnitt 6.2.1 verschlüsselt ein Zulieferer die genutzten Transportschlüssel nicht mit dem öffentlichen Schlüssel des KEK des CMS, sondern mit dem öffentlichen Schlüssel des KEK des Personalisierers. Als Folge hiervon entfällt das Umschlüsseln der kryptographischen Daten durch das CMS.

Abweichend von der Beschreibung in Abschnitt 6.2.1 gelten die folgenden Punkte:

Vor der Übertragung von kryptographischen Daten von einem Zulieferer an ein CMS muss der öffentliche Schlüssel und der Schlüsselname des KEK des Personalisierers an den Zulieferer übermittelt werden. Dabei muss die Authentizität des KEK gewährleistet werden. Siehe dazu auch die Ausführungen in Abschnitt 6.1.

Für den Zulieferer gilt:

Bei der Aufbereitung der kryptographischen Daten muss der Personalisierer die Vorgaben aus Abschnitt 5.3 berücksichtigen.

Der Transportschlüssel muss mit dem öffentlichen Schlüssel des KEK des Personalisierers verschlüsselt werden. Für die dabei verwendeten Verfahren müssen die Vorgaben aus Abschnitt 5.1.1 berücksichtigt werden.

Ggf. kann der Zulieferer die Daten direkt in entsprechende XML-Elemente `TransportKey`, `eGKCertificate` und `eGKKey` eingestellt und an das CMS übertragen werden. Eine andere Form der Übertragung kann aber bilateral zwischen CMS und Zulieferer abgestimmt werden.

Für das CMS gilt:

Das CMS muss die von einem Zulieferer erhaltenen (ggf. verschlüsselten) kryptographischen Daten einer eGK und die verschlüsselten Transportschlüssel ohne weitere Änderungen in den Personalisierungsauftrag einstellen. Ggf. (falls nicht bereits so von dem Zulieferer übertragen) müssen die Daten in die entsprechenden XML-Elemente `TransportKey`, `eGKCertificate` und `eGKKey` eingestellt werden.

Das CMS muss bei den in dem Personalisierungsauftrag enthaltenen Elemente `TransportKey` sicherstellen, dass deren Töchterelemente `EncryptedKey` in den Attributen `ID` unterschiedliche Referenzen haben. Falls ein entsprechendes Element bereits von einem Zulieferer angeliefert wurde, muss die Referenz ggf. geändert werden.

Das CMS muss bei den in dem Personalisierungsauftrag enthaltenen Elementen `eGKKey` in den zugehörigen Unterelementen `ds:RetrievalMethod` das Attribut `URI` die richtige Referenz auf den korrekten Transportschlüssel enthält. Falls ein entsprechendes Element bereits von einem Zulieferer angeliefert wurde, muss die Referenz ggf. angepasst werden.

Im Gegensatz zu Abschnitt 6.2.1 muss das CMS bei dieser Variante keine eigenen Transportschlüssel generieren und keine Daten ent- bzw. Verschlüsseln.

Für den Personalisierer gilt:

Keine Abweichungen zu der Variante in Abschnitt 6.2.1.

Vorteile dieser Variante sind:

- Der Kartenherausgeber kann frei entscheiden, ob die (bzw. welche) kryptographischen Daten selber erzeugt werden bzw. von einem Zulieferer bezogen werden.
- Der Kartenherausgeber hat die volle Kontrolle über die Zusammenstellung aller Daten eines Personalisierungsauftrags.
- Von einem Zulieferer verschlüsselt erhaltene kryptographische Daten müssen durch das CMS nicht umgeschlüsselt werden.
- Von dem Erzeuger eines kryptographischen Datums bis zum Personalisierer wird ein gesicherter Kanal aufgebaut, d.h. das CMS hat auch keine theoretischen Möglichkeiten, Kenntnis über die durch den Erzeuger verschlüsselten Daten zu erlangen. Dies kann insbesondere dann von

Bedeutung sein, falls die kryptographischen Daten zu einer Anwendung gehören, die nicht von dem Kartenherausgeber selber verantwortet wird.

Nachteile dieser Variante sind:

- Die Entscheidung, welcher Personalisierer beauftragt werden soll, muss bekannt sein bevor kryptographische Daten bei einem Zulieferer bestellt werden.
- Die von verschiedenen Zulieferern bezogenen verschlüsselten Daten einer einzelnen eGK sind mit unterschiedlichen Transportschlüsseln verschlüsselt.
- Der öffentliche Schlüssel des Personalisierers muss (inkl. Schlüsselnamen) authentisch durch das CMS an die einzelnen Zulieferer weitergeleitet werden.

6.2.3 Datenzusammenführung durch Kartenproduktion

Bei dieser Variante beauftragt der Kartenherausgeber einen Personalisierer im Sinne eines Generalunternehmers. Der Kartenherausgeber (d.h. sein CMS) steuert keine kryptographischen Daten zu der Personalisierung der eGKs bei.

Zunächst entscheidet der Personalisierer, welche kryptographischen Daten er in seinen Systemen selber erzeugen will und welche er von Zulieferern beziehen möchte. Ggf. wählt er die entsprechenden Zulieferer aus. Dies kann ggf. auch in Absprache mit seinem Auftraggeber (Kartenherausgeber) geschehen, der die Verantwortung für alle Prozesse und ihre Sicherheit hat..

Die Schnittstelle zwischen dem Personalisierer und den Zulieferern muss zwischen diesen bilateral festgelegt werden. Dabei müssen bezüglich der Sicherheit der übertragenen kryptographischen Daten die Anforderungen aus Kapitel 3 erfüllt werden. Als Grundlage für diese Schnittstelle können die Vorgaben aus Abschnitt 5.1 verwendet werden.

Vor der Übertragung von kryptographischen Daten von einem Zulieferer an den Personalisierer muss der öffentliche Schlüssel und der Schlüsselname des KEK des Personalisierers an den Zulieferer übermittelt werden. Dabei muss die Authentizität des KEK gewährleistet werden. Siehe dazu auch die Ausführungen in Abschnitt 6.1.

Für den Personalisierer gilt:

Nach der Personalisierung muss der Personalisierer einige der kryptographischen Daten der produzierten eGKs an das CMS des Kartenherausgebers als Teil der Rückmeldungen liefern. Welche Daten genau geliefert werden müssen, kann bilateral festgelegt werden. Tabelle 2 liefert einen Anhalt, welche Daten vom CMS benötigt werden.

Der Personalisierer generiert die für die Rückmeldungen benötigten Transportschlüssel. Dabei gibt es prinzipiell die beiden folgenden Möglichkeiten:

- Es wird nur ein Transportschlüssel für alle in einer Datei enthaltenen Rückmeldungen generiert. Dieser wird für das ggf. notwendige Verschlüsseln (und die zugehörige MAC-Sicherung) aller in den Rückmeldungen enthaltenen kryptographischen Daten aller enthaltenen eGKs eingesetzt. In diesem Fall

enthält in der Datei mit den Rückmeldungen nur das Element `gematikMSG` ein Tochterelement `TransportKey`, das den verschlüsselten Transportschlüssel enthält.

- Es wird ein Transportschlüssel pro in den Rückmeldungen enthaltener eGK generiert. Ein Transportschlüssel wird dann nur für das ggf. notwendige Verschlüsseln (und die zugehörige MAC-Sicherung) der kryptographischen Daten einer enthaltenen eGK eingesetzt. Dies ist das empfohlene Vorgehen. In diesem Fall enthält in der Datei mit den Rückmeldungen jedes enthaltene Element `PersoRueck` ein Tochterelement `TransportKey`, das den verschlüsselten Transportschlüssel enthält.

  In jedem Fall wird ein Transportschlüssel mit dem öffentlichen Schlüssel des KEK des CMS verschlüsselt und in ein Element `TransportKey` in den Personalisierungsauftrag eingestellt. Das Vorgehen dabei und der genaue Aufbau des Elements `TransportKey` sind in Abschnitt 5.1.1 beschrieben.

  Die kryptographischen Daten einer eGK müssen durch den Personalisierer gemäß den Vorgaben aus Abschnitt 5.3 aufbereitet werden und in ein Element `eGKCertificate` (Aufbau gemäß Abschnitt 5.1.2) bzw. `eGKKey` (Aufbau gemäß Abschnitt 5.1.3) in die Datei mit den Rückmeldungen eingestellt werden.

Für das CMS gilt:

Das CMS erhält eine Datei mit Rückmeldungen. Diese hat die XML-Struktur gemäß Abschnitt 5.2.

Alle in einem Element `TransportKey` enthaltenen Transportschlüssel müssen mit dem privaten Schlüssel des eigenen KEK entschlüsselt werden. Um den richtigen KEK zu bestimmen muss ggf. der (in dem zugehörigen Element `ds:KeyName` enthaltene) Schlüsselname ausgewertet werden.

Alle in einem Element `eGKKey` enthaltenen verschlüsselten Daten müssen mit dem korrekten Transportschlüssel entschlüsselt werden. Danach muss der MAC überprüft werden. Der korrekte Transportschlüssel wird über die Referenz in dem Attribut `URI` des zugehörigen Elements `ds:RetrivalMethod` bestimmt.

Falls das CMS ein kryptographisches Datum nach dem Entschlüsseln außerhalb eines HSM speichern will, muss dieses mit einem geeigneten Schlüssel und einem geeigneten Verfahren verschlüsselt werden. Die übergeordneten Sicherheitsanforderungen aus Kapitel 3 müssen dabei berücksichtigt werden.

Vorteile dieser Variante sind:

- Der Personalisierer kann frei (in Absprache mit dem Kartenherausgeber, der die Verantwortung für den Gesamtprozess hat)) entscheiden, ob (bzw. welche) kryptographischen Daten selber erzeugt werden bzw. von einem Zulieferer besorgt werden.
- Der Kartenherausgeber hat für die Kartenproduktion nur einen "Ansprechpartner", d.h. der Personalisierer arbeitet im Sinne eines Generalunternehmers.

- Das CMS muss selber keine Daten für die Personalisierung verschlüsseln.

Nachteile dieser Variante sind:

- Der Kartenherausgeber kann keine kryptographischen Daten selber erzeugen.
- Der Kartenherausgeber hat die Verantwortung für, aber nicht die volle Kontrolle über alle Zulieferer.

6.3 Sicherheitsanforderungen bei der eigentlichen Personalisierung

Die Vorgaben aus Kapitel 5 für die Verschlüsselung und MAC-Sicherung der geheimen kryptographischen Daten einer eGK sichern diese Daten bei ihrer Übertragung von dem CMS an den Personalisierer. Sie müssen in dem Sicherheitskonzept beschrieben und in dem Sicherheitsgutachten bewertet werden. Bevor der Personalisierer diese Daten in eine eGK einbringen kann, muss er diese mit dem Transportschlüssel entschlüsseln und danach für die Personalisierung aufbereiten. Diese Aufbereitung ist von dem konkreten Kartenbetriebssystem der eGK abhängig.

Die Absicherung der kryptographischen Daten durch die (Transport-) Verschlüsselung durch das CMS reicht nicht bis in die zu personalisierende eGK selber, sondern nur bis zu einem vorgelagerten System des Personalisierers für die Aufbereitung der Daten für die eigentliche Personalisierung. Eine solche durchgängige Absicherung bis in die Karte wäre wünschenswert, ist aber stark abhängig von dem Betriebssystem der Chipkarte. Für eine eGK können verschiedene Betriebssysteme zum Einsatz kommen. Im Rahmen der Spezifikation der eGK wurden keine einheitlichen Vorgaben für die Personalisierung der eGK festgelegt. Es ist daher nicht möglich, eine aus Sicht des CMS einheitliche Schnittstelle für die Aufbereitung der Daten zu spezifizieren, die gleichzeitig eine Absicherung der Daten bis in die Karte erreicht.

Falls das konkrete Kartenbetriebssystem eine Personalisierung verschlüsselter Daten zulässt, muss die Aufbereitung der Daten für die eigentliche Personalisierung ein Verschlüsseln und (ggf. eine MAC-Sicherung) mit einem (kartenindividuellen) Personalisierungsschlüssel beinhalten. Das Umschlüsseln der geheimen kryptographischen Daten von der Transportverschlüsselung des CMS auf die (kartenindividuelle) Verschlüsselung der Personalisierung muss in einem HSM geschehen. Die Sicherheitsanforderungen aus Kapitel 4 müssen berücksichtigt werden.

Falls das konkrete Kartenbetriebssystem für die eigentliche Personalisierung keine Verschlüsselung und MAC-Sicherung der Daten zulässt, muss die Sicherheit der kryptographischen Daten bei der eigentlichen Personalisierung durch andere Maßnahmen als durch das Umschlüsseln in einem HSM sichergestellt werden. Ein solches Vorgehen ist nur in Ausnahmefällen gestattet. Die getroffenen Sicherheitsmaßnahmen müssen in einem gesonderten Sicherheitskonzept des Personalisierers beschrieben werden und durch einen externen Gutachter bewertet werden. Der Personalisierer muss den Kartenherausgeber auf diese Besonderheit in Kenntnis setzen und das Sicherheitsgutachten vorlegen. Es muss sichergestellt sein, dass auch bei dem gewählten Vorgehen der Schutzbedarf „sehr hoch“ für die geheimen kryptographischen Daten nicht verletzt wird und die Sicherheitsvorgaben der gematik in jedem Fall eingehalten werden.

Anhang A

A1 – Abkürzungen

Kürzel	Erläuterung
C2C	Card to card
CAMS	Card Application Management System
CH	Card holder
CMS	Card Management System
CV	Card verifiable
FBZ	Fehlbedienzähler
HBA	Heilberufsausweis
HSM	Hardware Security Module
ICV	Initial Channing Value
KEK	Key Encryption Key
KGK	Key Generation Key
MAC	Message Authentication Code
PIN	Personal Identification Number
PIN.CH	PIN Card Holder: PIN zum Schutz freiwilliger Anwendungen
PIN.home	PIN zur Absicherung der Patientenrechte und der privaten Schlüssel für ENC und AUT
PKI	Public Key Infrastruktur
PUK	PIN Unblocking Key
QES	Qualifizierte Elektronische Signatur
SK	Secret Key
SMC	Security Module Card
VSDD	Versichertenstammdatendienst
XML	Extensible Markup Language
ZDA	Zertifizierungsdiensteanbieter

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI]	BSI (12.2005): BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 1.0
[gemeGK_PIN PUK]	gematik (26.10.2006): Einführung der Gesundheitskarte - Beschreibung der zulässigen PIN- und PUK-Verfahren für die eGK Version 0.9.0
[gemPers]	gematik (07.09.2006): Einführung der Gesundheitskarte – Übergabeschnittstelle für die Produktion der eGK, Version 1.1.1
[gemPKI-CVCGK]	gematik (21.06.2006): Einführung der Gesundheitskarte – PKI für CV-Zertifikate; Grobkonzept, Version 1.1.0
[gemPKI-Reg]	gematik (17.08.2006): Einführung der Gesundheitskarte – PKI für CV-Zertifikate; Registrierung einer CVC-CA der zweiten Ebene, Version 1.2.0
[gemSpec eGK-P1]	gematik (07.02.2006): Die Spezifikation elektronische Gesundheitskarte; Teil 1 – Kommandos, Algorithmen und Funktionen des Kartenbetriebssystems Version 1.1.0, www.gematik.de
[gemSpec eGK-P2]	gematik (07.09.2006): Die Spezifikation der elektronischen Gesundheitskarte ;Teil 2 – Anwendungen und anwendungsspezifische Strukturen

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	Version 1.2.1, www.gematik.de
[gemTSL-Reg]	gematik (Draft): Einführung der Gesundheitskarte - PKI für X.509-Zertifikate; Registrierung eines Trust Service Provider (TSP)
[gemTSL-SP_CP]	gematik (24.08.2006): Einführung der Gesundheitskarte - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten, Version 0.9.0
[gemX.509-eGK]	gematik (14.06.2006): Einführung der Gesundheitskarte - Festlegungen zu den X.509 Zertifikaten der Versicherten, Version 1.2.0
[gemX.509-pseu]	gematik (23.08.2006): Einführung der Gesundheitskarte - Festlegungen zu den pseudonymisierten X.509 Zertifikaten der Versicherten, Version 0.9.0
[gemX.509-TSL]	gematik (2005): Einführung der Gesundheitskarte - Festlegung einer einheitlichen X.509-Zertifikatsinfrastruktur (TSL) Version 1.0.0
[PKCS#1]	RSA Laboratories (06.2002): PKCS#1 v2.1: RSA Cryptography Standard, http://www.rsasecurity.com/rsalabs/node.asp?id=2125
[XMLEnc]	W3C (10.2002): XML Encryption Syntax and Processing