SRQ - Specification Related Question

SRQ-ID: 0906

Betrifft (wird vom FLS (optional vom Erfasser) ausgefüllt):

Themenkreis	Kartenmanagement
Schlagwort	Anpassung an die Personalisierung kryptographischer Daten auf der eGK
zu Dokument / Datei	[gemPers_Krypt]
Version	1.0.0
Bezug (Kap., Abschnitt, Tab., Abb.)	Kap. 2.5, 2.6.1, 3, 4, 5.1, 5.3, 6.1, A1 und A5

Stichwort: Anpassung an die Personalisierung kryptographischer Daten auf der eGK

Frage:

Welche Änderungen der Dokumentversion 1.0.0 ergeben sich durch Anpassung an die Personalisierung kryptographischer Daten auf der eGK?

Betrifft (wird vom PB ausgefüllt):

Gültig ab Release	0.5.2	Verbindlichkeit	ja
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☐ erfasst ☐ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☐ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Im Zuge der Anpassung des Release 0.5.2 an das R 2.3.4 wurden die folgenden Änderungen im [gemPers_Krypt] gegenüber der Dokumentversion 1.0.0 vorgenommen. Die Änderungen sind verbindlich und wurden in der Dokumentversion 1.1.0 umgesetzt. Die vorliegende SRQ beschreibt die funktionalen Änderungen.

Abs. 2.5:

Die Abgrenzung zwischen dem Dokument und dem übergreifenden Sicherheitskonzept [gemSiKo] wird deutlich beschrieben. Die Sicherheitsanforderungen aus [gemSiKo] sind für das Dokument normativ. Das Dokument beschreibt, wie diese durch die Betreiber umgesetzt werden.

In Bezug auf die zum Einsatz kommenden Algorithmen und die Längen der beteiligten Schlüssel sowie deren Gültigkeitsdauer werden durch [gemSpec_Krypt] und [gemSpec_eGK_P1] vorgegeben.

Grundsätzlich unterscheiden sich die Chipkarten der Teleinfrastruktur durch ihre Generationen. Für die Produktion der Chipkarten der Generation 0 gelten die Vorgaben aus der Version 1.0.0 dieses Dokuments. Die Vorgaben für die Chipkarten der Generation 1 ergeben sich aus der Dokumentversion plus dieser SRQ. Die Vorgaben für die Chipkarten der Generation 2 werden in dieser SRQ nicht behandelt.

In Bezug auf die Sicherheitsanforderungen ist die vorliegende Dokumentversion eine Ergänzung bzw. Präzisierung der Anforderungen aus den [gemPKI_CVCGK], [gemPKI_Reg] [gemTSP_SP_CP] und [gemX.509_TSL]. Zur Übersicht wurde daher ein Kapitel (3 Anforderungen), welches die Eingangsanforderungen auflistet, hinzugefügt.

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 folgende Tabelle enthält die vorläufig erfassten Eingangsanforderungen. Die Tabelle wird in einer Folgeversion nach der Abstimmung mit dem Anforderungsmanagement um weitere Eingangsanforderungen erweitert.

Tabelle 1: vorläufig erfasste Eingangsanforderungen

Quelle	Anforderungsnummer	Anforderungslevel	Beschreibung
[gemSiKo]	A_03189	MUSS	Die Systeme MÜSSEN jeden Versuch verhindern, einen Schlüssel unautorisiert auszulesen, zu verändern, zu ersetzen oder zu benutzen
[gemSiKo]	A_03164	MUSS	Die Berechnung von Schlüsseln MUSS mit Hilfe eines kryptographischen Algorithmus so erfolgen, dass • der berechnete Schlüssel ohne Kenntnis des für die Berechnung benutzten Schlüssels nicht einfacher bestimmt werden kann als ein zufällig erzeugter Schlüssel. • aus der Kenntnis des berechneten Schlüssels und der übrigen Inputdaten keine Informationen über den für die Berechnung benutzten Schlüssel abgeleitet werden können, ohne den zugrunde liegenden kryptographischen Algorithmus zu brechen.
[gemSiKo]	A_03197	MUSS	Wenn in sicherer Umgebung Schlüssel im Klartext transportiert werden, MÜSSEN zusätzlich zur Vertraulichkeit auch die Authentizität und Integrität der Schlüssel durch ein geeignetes kryptographisches Verfahren sichergestellt werden.

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 folgende Tabelle enthält die vorläufig erfassten Eingangsanforderungen. Die Tabelle wird in einer Folgeversion nach der Abstimmung mit dem Anforderungsmanagement um weitere Eingangsanforderungen erweitert.

Tabelle 1: vorläufig erfasste Eingangsanforderungen

Quelle	Anforderungsnummer	Anforderungslevel	Beschreibung
[gemSiKo]	A_03198	MUSS	Wenn Schlüssel in verschlüsselter Form verteilt werden, MUSS zusätzlich zur Vertraulichkeit auch die Authentizität und Integrität der Schlüssel durch ein geeignetes kryptographisches Verfahren sichergestellt werden. Das Verfahren MUSS auch erlauben, das Wiederverteilen alter Schlüssel zu erkennen.

Das Erzeugen qualifizierter Signaturen muss die Anforderungen aus SigV und SigG einhalten. Die Verantwortlichkeit für das Ausstellen des qualifizierten Zertifikats wurde festgelegt.

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 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.

Aktuell werden für die Chipkarten der Telematikinfrastruktur drei Generationen G0, G1 und G2 unterschieden. Die Vorgaben aus der vorliegenden Version dieses Dokuments gelten nur für die Produktion von eGKs der Generation G1. Für die Produktion von eGKs der Generation G0 gelten weiterhin die Vorgaben aus der Version 1.0.0 vom 20.12.2006 dieses Dokuments.

Bezüglich der Sicherheitsanforderungen stellt dieses Dokument ebenfalls eine Ergänzung und Präzisierung der Anforderungen aus 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.

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 die Anforderungen aus SigG [SigÄndG] und SigV [SigV01] eingehalten 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.

Abs. 2.6.1:

Die Schlüsselworte gemäß RFC2119 wurden eingefügt und durchgängig in der Dokumentversion umgesetzt.

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.

Kap. 3:

Die Basis für asymmetrische, symmetrische Kryptographie und die jeweiligen Schlüssellängen wurden für die Chipkartengenerationen 0 und 1 festgelegt. Die asymmetrische und symmetrische Kryptographie für die Chipkartengeneration 2 beruhen zwar auf der Basis von ECC bzw. AES-Verschlüsselungsfunktion, sie sind aber in der Dokumentversion nicht detailliert spezifiziert.

4 Kryptographische Daten ~~und Sicherheitsanforderungen~~

Aktuell werden für die Chipkarten der Telematikinfrastruktur die drei Generationen G0, G1 und G2 unterschieden. Bezüglich der Kryptographie legt die Generation einer Chipkarte dabei die

zu verwendenden Algorithmen und die Längen der beteiligten Schlüssel fest. Folgende Tabelle zeigt die aktuellen Vorgaben, welche aus dem übergreifenden Sicherheitskonzept zu entnehmen sind (siehe hierzu [gemSiKo#AnhF3.3.3]):

Tabelle 2: Unterscheidung der Kartengenerationen der Gesundheitstelematik

Generation	Basis für asymmetrische Kryptographie	Schlüssellänge für asymmetrische Kryptographie	Basis für symmetrische Kryptographie
G0	RSA	1024 – 2048	2TDES
G1	RSA	2048	3TDES
G2	elliptische Kurven (ECC)	ECC-256	AES-XXX

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

Anmerkung: Die konkreten Algorithmen die für die Kartengeneration G2 (Ausgabe ab etwa 2011), basierend auf elliptischen Kurven und AES, verwendet werden sollen, werden noch festgelegt. Für Elliptische Kurven und AES wird ECC-256 bzw. AES-128 (oder AES-256) vorgeschlagen (siehe hierzu [gemSiKo#AnhF3.3.3]).

Die Abkürzung CAMS wurde gemäß [gemPKI_Nota] in CMS in der Dokumentversion durchgängig ersetzt. Die Ersetzungen wurden in den Abschnitten 4.1 (und Tabelle 3), 4.2 (und Tabelle 4) und 6.1.3

4.1 Vorhandene kryptographische Daten

Tabelle 3: Übersicht der zur Personalisierung der eGK übertragenen geheimen kryprographische Daten

Bezeichner	Typ	Gespeichert in	Nutzung für
KGK.CMS.AUT (*1) KGK.CMS.ENC (*1)	Masterschlüssel symmetrisch	CMS	Ableiten der kartenindividuellen Schlüssel SK.CMS.AUT und SK.CMS.ENC
SK.CMS.AUT SK.CMS.ENC	kartenindividuell symmetrisch	CMS (*2) eGK	Authentikation zwischen eGK und CMS (inkl. Aushandlung Session-schlüssel)
KGK.VSDD.AUT (*1) KGK.VSDD.ENC (*1)	Masterschlüssel symmetrisch	VSDD	Ableiten der kartenindividuellen Schlüssel SK.VSDD.AUT und SK.VSDD.ENC

SK.VSDD.AUT SK.VSDD.ENC	kartenindividuell symmetrisch	VSDD (*2) eGK	Authentikation zwischen eGK und VSDD (inkl. Aushandlung Session-schlüssel)
KGK.VSDDCMS.AUT (*1) KGK.VSDDCMS.ENC (*1)	Masterschlüssel symmetrisch	CMS und VSDD	Ableiten der kartenindividuellen Schlüssel SK.VSDDCMS.AUT und SK.VSDDCMS.ENC
SK.VSDDCMS.AUT SK.VSDDCMS.ENC	kartenindividuell symmetrisch	CMS (*2) und VSDD (*2) eGK	Authentikation zwischen eGK und VSDD bzw. zwischen eGK und CMS (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	CMS eGK	Rücksetzen FBZ der PIN.CH
PIN.home	PIN	eGK	Benutzerauthentikation
PUK.home	PIN	CMS eGK	Rücksetzen FBZ der PIN.home
Geheimer herausgeber-spezifischer Zufallswert	Zufallswert (8 Byte)	CMS	Berechnung des Pseudonyms für das AUTN-Zertifikat ~~[gemX.509-pseu]~~ [gemX.509_eGK]

(*1): Die Masterschlüssel KGK.CMS.x, KGK.VSDD.x und KGK.VSDDCMS.x sind optional. Sie werden nur dann benötigt, falls die entsprechenden kartenindividuellen Schlüssel bei ihrer Generierung nicht zufällig erzeugt werden, sondern aus diesen Masterschlüsseln abgeleitet werden.

(*2): Die kartenindividuellen Schlüssel müssen im CMS 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.CMS.x, KGK.VSDD.x und KGK.VSDDCMS.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 an der Übertragung ~~Überträger~~ dieser privaten Schlüssel Beteiligten müssen über ihr Sicherheitskonzept nachweisen, dass sie diese privaten Schlüssel (nach der Personalisierung der Karte) nicht (mehr) gespeichert haben (siehe hierzu Abschnitt 5.1.2).

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_eGK~~-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.CMS.x, KGK.VSDD.x und KGK.VSDDCMS.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.

4.2 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:

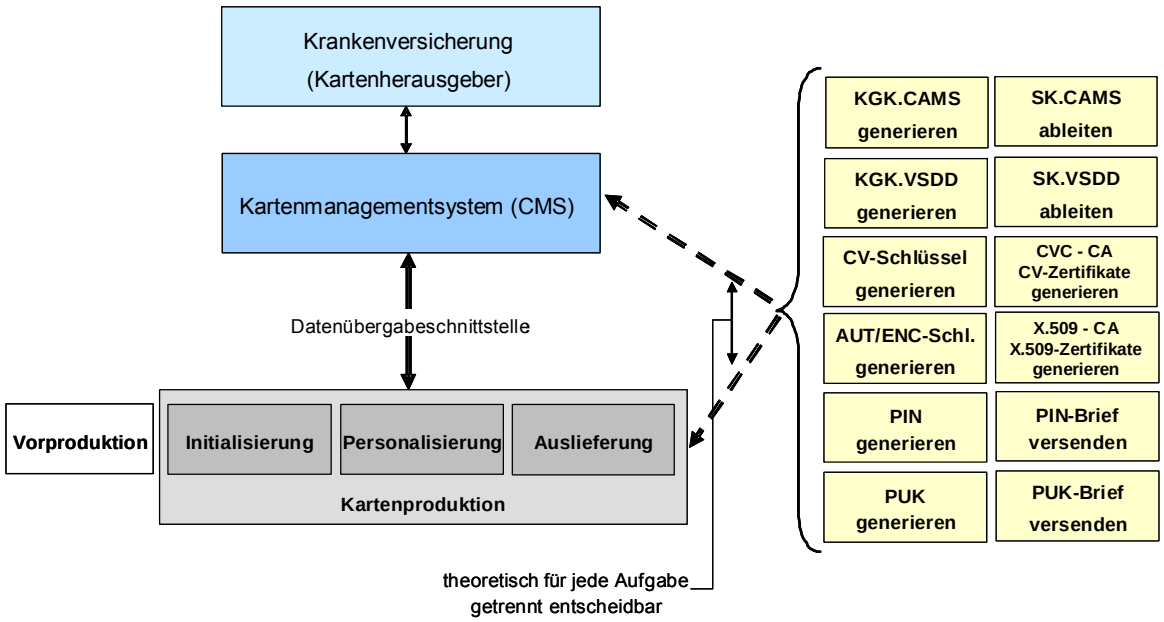

Abbildung 1 – Kartenproduktion: Beteiligte Organisationen/Rollen

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#5] 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.CMS.x

> SK.CMS.x ist ein kartenindividueller Schlüssel der eGK. Für die Ableitung wird ein Zugriff auf den Masterschlüssel KGK.CMS.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.VSDDCMS.x und der Ableitung von SK.VSDDCMS.x

> Es gelten die gleichen Anforderungen wie für das Generieren von KGK.CMS.x und für

das Ableiten von SK.CMS.x.

Generieren des Masterschlüssels und Ableitung der kartenindividuellen Schlüssel werden durch die gleichen Organisationen wie für KGK.CMS.x und SK.CMS.x übernommen.

4.2 Datenfluss bei der Kartenproduktion

Tabelle 4: Verteilung der kryptographischen Daten

	Kartenmanagement → Kartenproduktion	Kartenproduktion → Kartenmanagement
KGK.CMS.x generieren	KGK.CMS.x, nur falls Kartenproduktion die Schlüssel SK.CMS.x ableiten soll	KGK.CMS.x
SK.CMS.x ableiten/gener.	SK.CMS.x	SK.CMS.x, nur falls dieser kartenindividuell generiert wird
KGK.VSDD.x generieren	~~KGK.CAMS.x~~ KGK.VSDD.x nur falls Kartenproduktion die Schlüssel ~~SK.CAMS~~ SK.VSDD ableiten soll.	KGK.VSDD.x
SK.VSDD.x ableiten	SK.VSDD.x	SK.VSDD.x, nur falls dieser kartenindividuell generiert wird
KGK.VSDDCMS.x generieren	KGK.VSDDCMS.x, nur falls Kartenproduktion die Schlüssel SK.VSDDCMS.x ableiten soll	KGK.VSDDCMS.x
SK.VSDDCMS.x ableiten/gener.	SK.VSDDCMS.x	SK.VSDDCMS.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 an der Übertragung eines

Karte nicht (mehr) gespeichert haben (siehe hierzu Abschnitt 5.1.2).

6.1.3 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.CMS.AUT

KGK.CMS.ENC

SK.CMS.AUT

SK.CMS.ENC

KGK.VSDD.AUT

KGK.VSDD.ENC

SK.VSDD.AUT

SK.VSDD.ENC

KGK.VSDDCMS.AUT

KGK.VSDDCMS.ENC

SK.VSDDCMS.AUT

SK.VSDDCMS.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.CMS.x, KGK.VSDD.x oder KGK.VSDDCMS.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 0, 0 oder 0 aufbereitet werden.
- Das Element EncryptionMethod ist leer, hat aber das Attribut Algorithm, das den verwendeten Algorithmus angibt. Siehe hierzu den Hinweis nach dieser Aufzählung. ~~.='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 6.1.1.

Hinweis zum Verschlüsselungsverfahren:

Für die symmetrische Verschlüsselung der kryptographischen Daten MUSS ein Verfahren gemäß [gemSpec_Krypt#6.1.5] verwendet werden. Das Attribut Algorithm in dem Element EncryptionMethod MUSS entsprechend gesetzt werden.

Die Sicherheitsvorgaben für PIN.CH und PIN.home wurden aus [gemSiKo#AnhE] und [gemCMS_PINPUK#4] referenziert.

4.1 Vorhandene kryptographische Daten

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

Das übergreifende Sicherheitskonzept gibt für die Verwendung von PINs und zugehörigen PUKs an allen betroffenen Komponenten in der Telematikinfrastruktur Mindeststandards und Sicherheitsanforderungen vor [gemSiKo#AnhE]. Aus

technischer Sicht gibt es dafür verschiedene Verfahren, die jeweils unterschiedliche Vor- und Nachteile haben. Die von der gematik gestatteten PIN-Verfahren werden in [gemCMS_PINPUK#4] beschrieben.

~~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 (z.B. Daten der Protokollierung auf der eGK) erlangt werden kann. In einem solchen Fall muss bei der Produktion eine geheime (Transport- oder Echt-) PIN in die eGK eingebracht werden [gemCMS_PINPUK#4.5.2]. 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 [gemCMS_PINPUK#4.5.2]. 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.

Die Vorgaben für die Registrierung von X.509-CA und CVC-CA müssen gemäß [gemTSP_SP_CP] bzw. [gemPKI_Reg] erfüllt werden (Abs. 4.2).

4.2 Datenfluss bei der Kartenproduktion

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 gemäß [gemX.509-TSP#5] zugelassenen X.509-CA erzeugt und signiert werden. Der CA-Betreiber muss als Vorbedingung für diese Registrierung nachweisen, dass er die Anforderungen aus [gemTSL_SP_CP] erfüllt. ~~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_eGK ~~-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~~gemTSL_SP_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.

Die CVC-CA muss durch die gematik registriert sein und die Anforderungen aus [gemPKI_Reg] erfüllen.

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

Kap. 4

Die Vorgaben für das Sicherheitsniveau in Bezug auf die *Schutzbedarfsfeststellung*, die *Sicherheit geheimer kryptographischer Schlüssel*, die *Sicherheit von PINs und PUKs*, die *Authentizität einer eGK*, die *Schlüssellängen und Algorithmen*, die *Anforderung an ein HSM*, die *Protokollierung* und die *betriebliche Anforderungen* wurde gemäß der Umsetzung des RFC2119 (Verwendung geeigneter Schlüsselworte) und der entsprechenden Referenzierungen angepasst.

5.1 Vergaben für das Mindestniveau

5.1.1 Schutzbedarfsfeststellung

Der Schutzbedarf für die einzelnen kryptographischen Daten einer eGK wird durch das Sicherheitskonzept [gemSiKo#Anh.C2] vorgegeben.

Der Schutzbedarf für die kryptographischen Schlüssel (-paare), die für die Absicherung des Transports der Daten zwischen CMC und Personalisierer eingesetzt werden (Transportschlüssel und Key-Encrytion-Key) ergibt sich sinngemäß aus dem Schutzbedarf der kryptographischen Daten einer eGK mit dem höchsten Schutzbedarf.

~~Bezüglich des gesamten Prozesses der Produktion einer eGK wird der Schutzbedarf 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 5.1.4)~~

5.1 Vergaben für das Mindestniveau

5.1.2 Sicherheit geheimer kryptographischer Schlüssel

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

Es gelten die folgenden Anforderungen ([gemSiKo#Anh.F5.1]):

Ein geheimer Schlüssel (bei einem asymmetrischen Schlüssel das Schlüsselpaar) MUSS in einem dafür zugelassenen HSM (siehe Abschnitt 5.1.6) generiert werden.

Ein geheimer Schlüssel DARF ein HSM NICHT im 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 ausreichend sichere Authentifikation geschützt sein. Die Zugriffe MÜSSEN protokolliert werden, das Zugriffssystem MUSS ~~durch die gematik zugelassen sein~~ in dem Sicherheitskonzept (Abschnitt 5.2.1) beschrieben sein und durch den Sicherheitsgutachter (Abschnitt 5.2.2) bewertet werden.

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 Sicherheitskonzept 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. Ein typischer Anwendungsfall ist die Übergabe der privaten Schlüssel an den Personalisierer in der DÜS [gemPers]

5.1 Vergaben für das Mindestniveau

5.1.3 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 [gemFK_CMSPIN]).

Im Rahmen der Personalisierung einer eGK gelten für den Umgang mit geheimen Transport-PINs, Echt-PINs und PUKs die folgenden Anforderungen ([gemSiKo#Anh.E2]):

Geheime Transport-PINs, Echt-PINs und PUKs MÜSSEN in einem zugelassenen HSM (siehe Abschnitt 5.1.6) 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.

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. Beispiele hierfür sind u.a. die Nutzung und Verteilung der PINs/PUKs, die in [gemSiKo#AnhE1.2.4] bzw. [gemCMS_PIMPUK#4.5]

5.1 Vergaben für das Mindestniveau

5.1.4 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

5.1 Vergaben für das Mindestniveau

5.1.5 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_Krypt] ~~[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 zeitnah 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.

5.1 Vergaben für das Mindestniveau

5.1.6 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, wird eine entsprechende Bestätigung der Chipkarte als sichere Signaturerstellungseinheit (SSEE) durch die Bundesnetzagentur benötigt. ~~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. Mechanismenstärke (bzw. das angenommene Angriffspotential) müssen "hoch" sein.

Folgende Funktionen eines Produktions-HSM dürfen nur nach einer ausreichend sicheren 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~~ MUSS durch den Betreiber festgelegt werden. Sichergestellt werden muss dabei aber, dass das HSM nur nach erfolgter Authentikation genutzt werden kann [gemSiKo#AnhB4.5.4] A_02809.

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.

5.1 Vergaben für das Mindestniveau

5.1.7 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 Informationen zur Verfügung, um ihren Weg bis zum Wafer zurückverfolgen zu können.

5.1 Vergaben für das Mindestniveau

5.1.8 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.

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

Weitere Anpassungen der Anforderungen an die Sicherheitskonzepte und Sicherheitsgutachtung für die Umsetzung der Sicherheitsvorgaben und für die Einhaltung des Sicherheitsniveaus durch den Dienstbetreiber wurden vorgenommen.

5.2 Umsetzung der Sicherheitsanforderungen

Die Einhaltung aller in Abschnitt 5.1 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.

5.2.1 Anforderungen an ein Sicherheitskonzept

Der Betreiber eines Systems, das an der Personalisierung kryptographischer Daten einer eGK beteiligt ist, MUSS (falls durch den Kartenherausgeber verlangt) 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 5.1.1 auszugehen.

Der Betreiber MUSS sich bezüglich Umfang und Aufbaus seines Sicherheitskonzepts an den Vorgaben für die Sicherheitskonzepte der Dienstebetreiber aus [gemSiKo#8.6.2] orientieren.

5.2.2 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 durch die gematik anerkannten Gutachter erstellt werden. ~~Aktuell werden die durch das BSI akkreditierten Prüfstellen als solche angesehen (siehe http://www.bsi.de/zertifiz/zert/pruefst.htm).~~ Die gematik veröffentlicht die Liste der anerkannten Gutachter unter www.gematik.de. 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.

Kap. 5

Das asymmetrische Verschlüsselungsverfahren für den Transportschlüssel wurde angepasst und entsprechend auf [gemSpec_Krypt] verwiesen (Kap. 5.1.1).

6.1.1 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`, das den verwendeten Algorithmus angibt. Siehe hierzu den Hinweis nach dieser Aufzählung. ~~='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:

Für die asymmetrische Verschlüsselung des Transportschlüssels MUSS ein Verfahren gemäß [gemSpec_Krypt#6.1.6] verwendet werden. Das Attribut `Algorithm` in dem Element `EncryptionMethod` MUSS entsprechend gesetzt werden.

~~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 7.

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.

Die Bezeichnungen für die Verschlüsselung und MAC-Sicherung durch einen Transportschlüssel T wurden angepasst. Es betreffen die Bezeichnungen für ENC-T(a,B) und MAC-T(B) (Abs. 5.3).

Die Anpassung der Spezifikation für die Verschlüsselung und MAC-Sicherung symmetrischer (3TDES), asymmetrischer Schlüssel,CV-Zertifikate, PINs und PUKs und geheimer Zufallswerte einer eGK der Generation 1 wurde in der vorliegenden Dokumentversion vorgenommen (Abs. 5.3.1 – 5.3.5).

6.3 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): Symmetrische Verschlüsselung von B mit ICV a und dem Transportschlüssel T. Es MUSS ein Verfahren gemäß [gemSpec_Krypt#6.1.5] verwendet werden. ~~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. Für die Berechnung des MAC MUSS ein Verfahren gemäß [gemSpec_Krypt#6.9] verwendet werden. ~~Verwendet wird Triple-DES mit ICV a und Padding '80 00 … 00', wobei in jedem Fall mindestens ein Padding-Byte verwendet wird.~~

6.3.1 Symmetrische Schlüssel

Symmetrische Schlüssel einer eGK der Generation G1 sind gemäß [gemSpec_eGK_P1] ~~16~~ 24 Byte lange (3-Key) Triple-DES-Schlüssel. Ein solcher symmetrischer Schlüssel K wird mit einem Transportschlüssel T wie folgt verschlüsselt und MAC gesichert:

M = MAC-T (K) ~~MAC-T (0, K)~~

Kryptogramm = ENC-T (rnd, '80 18 K 8E xx M') mit 'xx' = Länge des MAC (hex-kodiert) bei dem genutzten Verfahren gemäß [gemSpec_Krypt#6.9]. ~~ENC-T (0, '80 10 K 8E 08 M')~~

Der ICV rnd ~~0~~ besteht dabei aus n zufällig gewählten Bytes. Die Länge n des ICV ist abhängig von der Blocklänge des Verschlüsselungsverfahrens gemäß [gemSpec_Krypt#6.1.5]. ~~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'~~ rnd | Kryptogramm

6.3.2 Asymmetrische Schlüsselpaare

Asymmetrische Schlüsselpaare einer eGK der Generation G1 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 5: TLV-Struktur für einen privaten Schlüssel

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

'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 6: 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 (S) ~~MAC-T (0, S)~~

Kryptogramm = ENC-T (rnd, 'B2 82 xx xx S 8E yy M') mit 'yy' = Länge des MAC (hex-kodiert) bei dem genutzten Verfahren gemäß [gemSpec_Krypt#6.9]. ~~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 rnd besteht dabei aus n zufällig gewählten Bytes. Die Länge n des ICV ist abhängig von der Blocklänge des Verschlüsselungsverfahrens gemäß [gemSpec_Krypt#6.1.5]. ~~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'~~ rnd | Kryptogramm

6.3.3 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#8.1.3] 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.

6.3.4 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 (B) ~~MAC-T (0, B)~~

Kryptogramm = ENC-T (rnd, '80 08 B 8E xx M') mit 'xx' = Länge des MAC (hex-kodiert) bei dem genutzten Verfahren gemäß [gemSpec_Krypt#6.9]. ~~ENC-T (0, '80 08 B 8E 08 M')~~

Der ICV rnd besteht dabei aus n zufällig gewählten Bytes. Die Länge n des ICV ist abhängig von der Blocklänge des Verschlüsselungsverfahrens gemäß [gemSpec_Krypt#6.1.5]. ~~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'~~ rnd | Kryptogramm

6.3.5 Herausgeberspezifischer geheimer Zufallswert

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

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

M = MAC-T (RND) ~~MAC-T (0, RND)~~

Kryptogramm = ENC-T (rnd, '80 08 RND 8E xx M')) mit 'xx' = Länge des MAC (hex-kodiert) bei dem genutzten Verfahren gemäß [gemSpec_Krypt#6.9]. ~~ENC-T (0, '80 08 RND 8E 08 M')~~

Der ICV rnd besteht dabei aus n zufällig gewählten Bytes. Die Länge n des ICV ist abhängig von der Blocklänge des Verschlüsselungsverfahrens gemäß [gemSpec_Krypt#6.1.5]. ~~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'~~ rnd | Kryptogramm

Kap. 6

Die Länge des Transportschlüssels wird aus [gemSpec_Krypt] referenziert. Die Geheimhaltung dieses Schlüssels wird durch ein asymmetrisches RSA-Schlüsselpaar (KEK) realisiert. Das notwendige Management des KEK wird aus [gemSiKo#AnhF5.1.2] referenziert. Die Spezifikation der Mindestlänge wird auf [gemSpec_Krypt#5.1.1.7] verwiesen (Abs. 6.1).

7 Vorgehen bei der Datenaufbereitung

7.1 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 Dieser wird für das symmetrische Ver- und Entschlüsseln der eigentlichen eGK-Daten verwendet. Die Länge des Transportschlüssels hängt von dem Verschlüsselungsverfahren ab, das gemäß [gemSpec_Krypt#6.1.5] gewählt werden MUSS.

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 [gemSiKo#Anh.F5.1.2] sicher zu erzeugen und sicher aufzubewahren.

Für den Umgang mit diesen Schlüsseln gelten die gleichen Anforderungen aus Abschnitt 5.1 wie für die kryptographischen Daten einer eGK.

Für die Schlüssellänge gilt dabei folgende Konkretisierung:

Ein KEK MUSS eine Mindestlänge ~~von 2048 Bit~~ haben, die die Vorgaben aus [gemSpec_Krypt#5.1.1.7] erfüllt.

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 0) kann es notwendig sein, dass auch ein Zulieferer von kryptographischen Daten den öffentlichen Schlüssel des Personalisierers erhält (siehe Variante in Abschnitt 0). 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.

Weitere Anpassung gemäß der Umsetzung des RFC2119 sowie Änderungen in Bezug auf die Referenzierungen und Begrifflichkeit sind aus der nachstehenden Anlage zu entnehmen

7.2 Modelle für die Zusammenarbeit

Wie in Abschnitt 0 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 0), während er die Daten bei der zweiten Variante so verschlüsselt, dass nur der Personalisierer diese entschlüsseln kann (siehe Abschnitt 0).

Bei der zweiten Alternative (siehe Abschnitt 0) 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 6 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.

7.2.1 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 5 erfüllt werden. Als Grundlage für diese Schnittstelle können die Vorgaben aus Abschnitt 6.1 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 7.1.

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 0 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 6.1.1 beschrieben.

Die kryptographischen Daten einer eGK müssen durch das CMS gemäß den Vorgaben aus Abschnitt 6.3 aufbereitet werden und in ein Element `eGKCertificate` (Aufbau gemäß Abschnitt 6.1.2) bzw. `eGKKey` (Aufbau gemäß Abschnitt 6.1.3) in den Personalisierungsauftrag eingestellt werden.

Für den Personalisierer gilt:

Der Personalisierer erhält einen Auftrag mit der XML-Struktur gemäß Abschnitt 6.1.

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.

7.2.2 Datenzusammenführung durch CMS

Diese Variante ist ähnlich zu der in Abschnitt 0 beschriebenen Variante. Abweichend zu

Abschnitt 0 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 0 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 öffentlichen Schlüssels des KEK gewährleistet werden (siehe Datenklasse DK 09 in [gemSiKo#7.3] für den Schutzbedarf). Siehe dazu auch die Ausführungen in Abschnitt 7.1.

Für den Zulieferer gilt:

Bei der Aufbereitung der kryptographischen Daten muss der Personalisierer die Vorgaben aus Abschnitt 0 berücksichtigen.

Der Transportschlüssel muss mit dem öffentlichen Schlüssel des KEK des Personalisierers verschlüsselt werden. Für die dabei verwendeten Verfahren müssen die Vorgaben aus Abschnitt Tabelle 4 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 0 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 0.

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.

7.2.3 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 5 erfüllt werden. Als Grundlage für diese Schnittstelle können die Vorgaben aus Abschnitt 6.1 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 öffentlichen Schlüssels des KEK gewährleistet werden (siehe Datenklasse DK 09 in [gemSiKo#7.3] für den Schutzbedarf). Siehe dazu auch die Ausführungen in Abschnitt 7.1.

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 4 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 6.1.1 beschrieben.

Die kryptographischen Daten einer eGK müssen durch den Personalisierer gemäß den Vorgaben aus Abschnitt 6.3 aufbereitet werden und in ein Element eGKCertificate (Aufbau gemäß Abschnitt 6.1.2) bzw. eGKKey (Aufbau gemäß Abschnitt 6.1.3) 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 6.2.

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 5 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.

7.3 Sicherheitsanforderungen bei der eigentlichen Personalisierung

Die Vorgaben aus Kapitel 6 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 5 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 Vertraulichkeit der geheimen kryptographischen Daten nicht verletzt wird und die Sicherheitsvorgaben der gematik in jedem Fall eingehalten werden.

Abschließend wurden die A1 – Abkürzungen und A5 – Referenzierte Dokumente angepasst bzw. ergänzt.

A1 – Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
C2C	Card to card
CAMS	Card Application Management System
CH	Card holder

Kürzel	Erläuterung
CMS	Card Management System
CV	Card verifiable
DES	Ein veraltetes symmetrisches Verschlüsselungsverfahren (Data Encryption Standard)
2TDES	Dreifach hintereinander verkettete Ver-/Entschlüsselung gemäß DES mit einem Schlüssel der gesamten Länge 112 Bit (2-Key Triple-DES)
3TDES	Dreifach hintereinander verkettete Ver-/Entschlüsselung gemäß DES mit einem Schlüssel der gesamten Länge 168 Bit (3-Key Triple-DES)
ECC	Elliptische Kurve
ECC-256	Elliptische Kurve mit einer Kurvengröße von 256 Bit
DÜS	Datenübergabeschnittstelle
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
SigG	Signaturgesetz
SigV	Signaturverordnung
SK	Secret Key
SMC	Security Module Card
VSDD	Versichertenstammdatendienst
XML	Extensible Markup Language
ZDA	Zertifizierungsdiensteanbieter

A5 – Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik. Der mit dem vorliegenden Dokument korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen, die im Rahmen des Vorhabens zur Einführung der Gesundheitskarte veröffentlicht werden, wird pro Release in einer

Dokumentenlandkarte definiert. Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Die jeweils gültige Version und das Freigabedatum der aufgeführten gematik-Dokumente entnehmen Sie bitte der von der gematik veröffentlichten Dokumentenlandkarte (aktuell [gemDokLK_2.3.4]), wobei jeweils der aktuellste Releasestand maßgeblich ist, in dem die vorliegende Version aufgeführt wird. Zur Unterstützung der Zuordnung wird in der Dokumentenlandkarte im Kapitel 4 eine Übersicht über die Dokumentenversionen und deren Zuordnung zu den verschiedenen Releases bereitgestellt.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemDokLK_2.3.4]	gematik: Einführung der Gesundheitskarte – Dokumentenlandkarte Releasestand 2.3.4 – Online Feldtest 10.000 Festlegung der Versionsstände
[gemFK_CMSPIN]	gematik: Einführung der Gesundheitskarte – Beschreibung der zulässigen PIN- und PUK-Verfahren für die eGK
[gemPers]	gematik : Einführung der Gesundheitskarte – Übergabeschnittstelle für die Produktion der eGK,
[gemPKI-CVCGK]	gematik: Einführung der Gesundheitskarte – PKI für CV-Zertifikate; Grobkonzept
[gemPKI_Nota]	gematik: Einführung der Gesundheitskarte – Festlegungen zu den Notationen von Schlüsseln und Zertifikaten kryptographischer Objekte
[gemPKI-Reg]	gematik: Einführung der Gesundheitskarte – PKI für CV-Zertifikate; Registrierung einer CVC-CA der zweiten Ebene,
[gemSiKo]	gematik: Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur
[gemSpec_eGK_P1]	gematik: Einführung der Gesundheitskarte – Die Spezifikation der elektronischen Gesundheitskarte; Teil 1 – Spezifikation der elektrischen Schnittstelle
[gemSpec_eGK_P2]	gematik: Einführung der Gesundheitskarte – Die Spezifikation der elektronischen Gesundheitskarte ; Teil 2 – Grundlegende Applikationen
[gemSpec_Krypt]	gematik: Einführung der Gesundheitskarte – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur,
[gemX.509-TSP]	gematik: Einführung der Gesundheitskarte - PKI für X.509-Zertifikate; Registrierung eines Trust Service Provider (TSP)
[gemTSL-SP_CP]	gematik: Einführung der Gesundheitskarte - gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten
[gemX.509_eGK]	gematik: Einführung der Gesundheitskarte - Festlegungen zu den X.509 Zertifikaten der Versicherten
[gemX.509-TSL]	gematik: Einführung der Gesundheitskarte - Festlegung einer einheitlichen X.509-Zertifikatsinfrastruktur (TSL)

Weitere Referenzen

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-TR03116]	BSI TR-03116 (23.03.2007): Technische Richtlinie für die eCard-Projekte der Bundesregierung Version: 1.0 http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf (Zuletzt geprüft am 17.06.2008)
[PKCS#1]	RSA Laboratories (06.2002): PKCS#1 v2.1: RSA Cryptography Standard, http://www.rsasecurity.com/rsalabs/node.asp?id=2125. (Zuletzt geprüft am 17.06.2008)
[SP800-38B]	NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001 Edition
[SigÄndG]	Bundesgesetzblatt I (2005), S.2: 1.Gesetz zur Änderung des Signaturgesetzes
[SigV01]	Bundesgesetzblatt I (2001), S. 3074: Verordnung zur elektronischen Signatur – SigV
[XMLEnc]	W3C (10.2002): XML Encryption Syntax and Processing