Einheitliche Methoden der Informationssicherheit

Dokumentation von Schlüsselmaterial in der Telematikinfrastruktur

Version:	1.1.0
Revision:	\main\rel_online\20
Stand:	30.05.2013
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemMeth_Schlüssel]

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung Kommentare LA

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	15.10.12		freigegeben	gematik
			Einarbeitung Kommentare LA	P77
1.1.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.1.0	06.06.13		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Dem Umgang mit Schlüsselmaterial kommt eine zentrale Bedeutung zu. Auf das Kerckhoffssche Prinzip von 1883 [Kerck-1883] geht zurück, dass die Sicherheit eines kryptographischen Systems im praktischen Einsatz genau nur auf der Geheimhaltung der verwendeten geheimen bzw. privaten kryptographischen Schlüssel basieren darf. Die nachfolgende Methode gibt Vorgaben, wie die Verwendung von Schlüsselmaterial in der Telematikinfrastruktur (TI) dokumentiert werden muss. Sie trägt damit zur Qualitätssicherung der Spezifikationen und Sicherheitskonzeptionen hinsichtlich der verwendeten kryptographischen Verfahren bei.

Die Methode hat zwei Ziele:

1. Der fachgerechte Umgang mit kryptographischem Schlüsselmaterial soll gefördert werden und für Dritte (bspw. Sicherheitsgutachter) leichter nachvollziehbar sein. Die Mechanismenstärke von kryptographischen Verfahren in der TI kann maximal so gut sein, wie die Sorgfalt beim Umgang mit dem entsprechenden Schlüsselmaterial.

2. Bei einer späteren Erweitung der Spezifikation soll leicht ermittelbar sein, welchen Verwendungszweck spezielle Schlüssel haben (also welche Sicherheitsleistung sie erbringen müssen) und insbesondere, für was sie nicht noch zusätzlich verwendet werden dürfen. Auch soll leicht auffindbar sein, in welchen Umgebungen sie im Klartext gespeichert werden können bzw. welche Umgebungsanforderungen beim Umgang mit dem Schlüsselmaterial gestellt werden müssen.

Der gesamte Lebenszyklus des Schlüsselmaterials muss genau betrachtet werden: von der sicheren Erzeugung, über die Speicherung und Verwendung, bis hin zur sicheren Löschung. In jeder Lebensphase muss geregelt sein, wer für das Schlüsselmaterial verantwortlich ist und wie dessen Schutzbedarf sichergestellt wird. Bevor das Material erzeugt wird, muss genau festgelegt werden, wie lange es maximal verwendet werden darf und zu genau welchem Zwecke.

Die Methode muss in der Spezifikationsphase einer Fachanwendung und der TI-Plattform angewandt und schrittweise verfeinert werden. Sollten sich in einer späteren Phase Änderungen an der Architektur oder anderen wesentlichen Bestandteilen der Fachanwendungen oder der TI-Plattform ergeben, muss die Methodik erneut angewendet oder aktualisiert werden, um sicher zu gehen, dass die geforderte Sicherheitsleistung immer noch erbracht werden kann.

Wenn Systeme später erweitert werden, ist eines der häufigsten Probleme bei kryptographischen Verfahren, dass Schlüsselmaterial zusätzlich zum ursprünglichen Einsatzzweck noch für andere Zwecke verwendet wird. Damit Sicherheitsprobleme vermieden werden, muss klar beschrieben sein, wofür erzeugtes Schlüsselmaterial eingesetzt werden darf.

Die nachfolgende Grafik zeigt die Einordnung der Methode in die „Einheitlichen Methoden zur Informationssicherheit“ in der Telematikinfrastruktur:

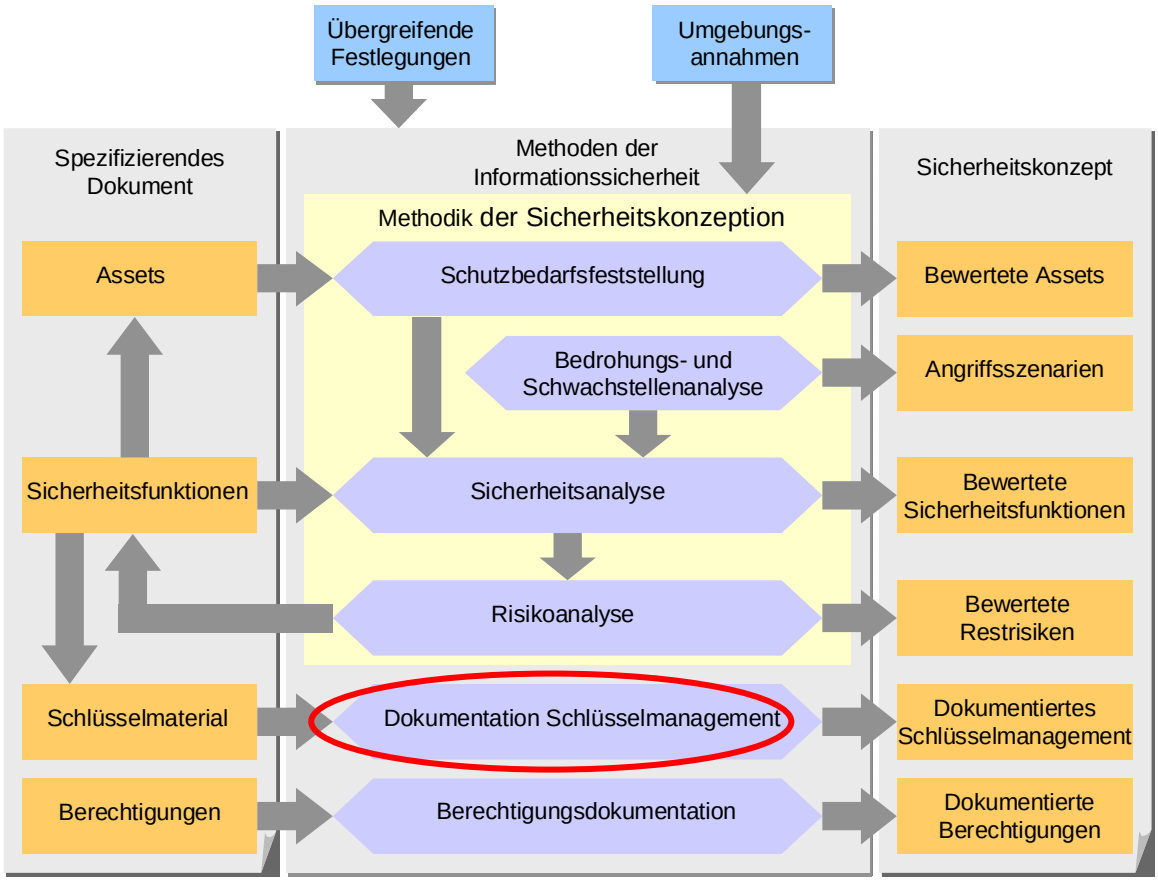

Abbildung 1: Einordnung der vorliegenden Methode

Das Ergebnis der vorliegenden Methode sind spezifische Angaben zum Lebenszyklus der verwendeten Schlüssel.

Die Ergebnisdarstellung erfolgt im jeweiligen Spezifikationsdokument, das den Schlüssel einführt.

1.2 Zielgruppe

Die vorliegende Methodik richtet sich an alle Personen, die Schlüsselmaterial in der Telematikinfrastruktur spezifizieren oder deren Einsatz bewerten.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren werden durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

1.4 Abgrenzungen

Das Dokument betrachtet kein konkretes Schlüsselmaterial.

Anhand eines Beispiels wird die Anwendung der Methode aufgezeigt. Das verwendete Beispiel hat keinen Einfluss auf die Ausgestaltung der TI.

1.5 Methodik

In der Schlüsseldokumentation werden keine Anforderungen definiert. Dies erfolgt in den Spezifikationsdokumenten.

2 Methodenbeschreibung

Damit die in der Telematikinfrastruktur genutzten kryptographischen Verfahren die Sicherheitsleistung erbringen können, die von ihnen erwartet wird, ist der Umgang mit dem Schlüsselmaterial, wie nachfolgend beschrieben, zu dokumentieren. Damit wird sichergestellt, dass alle Phasen des Lebenszyklus eines Schlüssels berücksichtigt wurden.

2.1 Generelle Angaben

Die nachfolgenden generellen Angaben bezüglich eines Schlüssels beschreiben u. a. dessen Verwendungszweck und seine technische Bezeichnung.

Tabelle 1: Generelle Angaben

Angaben zum Schlüssel	Erläuterung
Kurzbezeichnung des Schlüsselmaterials	Technische Bezeichnung des Schlüssels
Einsatzbereich	In welcher Komponente / Dienste etc. wird der Schlüssel verwendet.
Beschreibung des Nutzungszwecks des Schlüssels	Zu welchem Zweck (z.B. Verschlüsselung von xyz) wird der Schlüssel verwendet?
Typ des Schlüsselmaterials	Art des Schlüssels, z.B. „privater Schlüssel eines RSA-Schlüsselpaares“
Anwendung in welchem Sicherheitsverfahren	Welches Sicherheitsverfahren verwendet den Schlüssel (Algorithmus)?
ggf. Zuordnung zu einer PKI	Aus welcher PKI stammt der Schlüssel bzw. welche PKI bestätigt den Schlüsselinhaber?
Maximale Gültigkeitsdauer / typische Gültigkeitsdauer	Angabe der Gültigkeitsdauer des Schlüssels
Schutzbedarf	Der Schutzbedarf kann aus der Methodik zur Schutzbedarfsfeststellung übernommen und an dieser Stelle dokumentiert werden.

Tabelle 2: Verantwortlichkeiten und Schutz

Eigenschaft	Erläuterung
Verantwortlicher	Angabe des Hauptverantwortlichen für den Schlüssel (i.d.R. der Schlüsselbesitzer)
Zugriffsrechte	Angabe der Berechtigten Rollen zur Verwendung des Schlüssels
Zugriffsschutz	Angabe der Schutzmechanismen für den Schlüssel

2.2 Angaben zum Lebenszyklus

Der Lebenszyklus von kryptographischem Material wird im Anhang A3 in Anlehnung an ISO 11770 [ISO-11770] beschrieben. Folgende Punkte sind in Bezug darauf zu erläutern.

Tabelle 3: Angaben zum Lebenszyklus

Phase	Erläuterung / Prozess	Rolle	Einsatzumgebung
Initialisierungsphase			
Erzeugung	WIE? (ggf. Referenz auf Prozessbeschreibung) Backup erforderlich? [ja/nein]	Verant-wortliche Rolle	Annahmen / Anforde-rungen an die Umge-bung, in der der Vor-gang stattfindet
Schlüsselbackup	WIE? (ggf. Referenz auf Prozessbeschreibung) Backup erforderlich? [ja/nein]	Verant-wortliche Rolle	Annahmen / Anforde-rungen an die Umge-bung, in der der Vor-gang stattfindet
Registrierung	Notwendig? [ja/nein] Name der Registrierungsstelle (ggf. Referenz auf Prozessbeschreibung)	Verant-wortliche Rolle	Annahmen / Anforde-rungen an die Umge-bung, in der der Vor-gang stattfindet
Erzeugung eines Schlüssel-zertifikats	Notwendig? [ja/nein] Wo wird das Zertifikat erzeugt und unter Verwendung welches Schlüssels (ggf. Referenz auf Prozessbeschreibung)	Verant-wortliche Rolle	Annahmen / Anforde-rungen an die Umge-bung, in der der Vor-gang stattfindet
Verteilung	WIE? (ggf. Referenz auf Prozessbeschreibung)	Verant-wortliche Rolle	Anforderungen für die Schlüsselverteilung (insb. Schutzmaß-nahmen)
Betriebsphase			
Installation	WIE? (ggf. Referenz auf Prozessbeschreibung) Name des Systems, in dem der Schlüs-selt installiert ist	Verant-wortliche Rolle	Annahmen / Anforde-rungen an die Umge-bung, in der der Vor-gang stattfindet
Speicherung	WO (Speicherort)? Backup vorhanden? [ja/nein] Gleiche Angaben erforderlich	Verant-wortliche Rolle	Annahmen / Anforde-rungen an die Umge-bung, in der der Vor-gang stattfindet
Ableitung	Zulässig? [ja/nein] (ggf. Referenz auf Prozessbeschreibung sowie Angabe des Verfahrens)	Verant-wortliche Rolle	Annahmen / Anforde-rungen an die Umge-bung, in der der Vor-gang stattfindet
Aufheben der Registrierung / Entzug des Zertifikats	Zulässig / Möglich? [ja/nein] WIE? (ggf. Referenz auf Prozessbeschreibung)	Verant-wortliche Rolle	-

	Gründe: (Angabe möglicher Gründe die zur Aufhebung / Entzug führen)		
Suspendierung	Zulässig / Möglich? [ja/nein] WIE? (ggf. Referenz auf Prozessbeschreibung) Gründe: (Angabe möglicher Gründe für eine Suspendierung)	Verantwortliche Rolle	-
Reaktivierung	Zulässig / Möglich? [ja/nein] WIE? (ggf. Referenz auf Prozessbeschreibung) Gründe: (Angabe möglicher Gründe für eine Reaktivierung)	Verantwortliche Rolle	-
Sperrung	Zulässig / Möglich? [ja/nein] WIE? (ggf. Referenz auf Prozessbeschreibung) Gründe: (Angabe möglicher Gründe für eine Sperrung)	Verantwortliche Rolle	-
Nach-Betriebsphase			
Archivierung	Zulässig? [ja/nein] WO? (Speicherort und ggf. Schutzmaßnahmen auflisten) WIE LANGE (Datum)?	Verantwortliche Rolle	Annahmen / Anforderungen an die Umgebung, in der der Vorgang stattfindet
Zerstörungsphase			
Löschung / Zerstörung	WIE? (ggf. Referenz auf Prozessbeschreibung)	Verantwortliche Rolle	Annahmen / Anforderungen an die Umgebung, in der der Vorgang stattfindet

2.3 Notfallmaßnahmen bei Kompromittierung

Hinsichtlich der Notfallmaßnahmen bei einer Kompromittierung eines Schlüssels sind folgende Punkte zu dokumentieren:

Tabelle 4: Notfallmaßnahmen bei Kompromittierung

Prozess	Beschreibung	Verantwortlicher
Erfassung der Kompromittierung		Rolle
	WIE? (ggf. Referenz auf Prozessbeschreibung)	
Maßnahmen zur Schadensbegrenzung im Falle der Kompromittierung		Rolle
	WAS? (ggf. Referenz auf Prozessbeschreibung) Welche Maßnahmen werden ergriffen, wenn eine Kompromittierung des Schlüssels vermutet wird bzw. vorliegt? Gibt es ein Notfallkonzept? Gibt es ein Notfallmanagement (bspw. als Bestandteils eines ISMS)?	

2.4 spezifische Maßnahmen zum Schutz der Schlüssel

Die Anwendung der Methode hat gezeigt, dass es u. U. hilfreich ist, einige Maßnahmen gesondert im Rahmen der Dokumentationsmethode zu dokumentieren. Der Spezifikateur kann selbst entscheiden, ob dies in seinem konkreten Fall hilfreich ist. Wenn ja, sollte folgende Tabelle verwendet werden.

Tabelle 5: Umsetzung Schutzbedarf des Schlüssels

Vorkommen des Schlüssels	Einsatzumgebung	Maßnahmenbeschreibung
Erläuterung der konkreten Einsatzumgebung x (Freitext)	Einsatzumgebung x kategorisiert nach Anhang A2	Maßnahmenbeschreibung 1
Erläuterung der konkreten Einsatzumgebung y (Freitext)	Einsatzumgebung y kategorisiert nach Anhang A2	Maßnahmenbeschreibung 2
usw.		

2.5 Schlüsselmaterial der TI-Plattform

Falls eine Anwendung (oder ein Produkttyp)[1] kryptographische Schlüssel verwenden will, muss sie sicherstellen, dass der Schutzbedarf des Schlüsselmaterials während seines gesamten Lebenszyklus erfüllt wird. Für selbst erzeugtes Schlüsselmaterial (im Sinne durch die Anwendung spezifiziertes) muss die Anwendung Maßnahmen zum Schutz des Schlüsselmaterials spezifizieren. Die Anwendung muss den gesamten Lebenszyklus[2] anhand der in diesem Dokument beschrieben Methode dokumentieren (und im spezifischen Sicherheitskonzept - insbesondere Sicherheitsanalyse und Risikoanalyse - die Eignung der Maßnahmen nachweisen).

[1] In diesem Abschnitt gelten Aussagen für „eine Anwendung“ analog auch für beliebige Produkttypen der TI.
[2] siehe Anhang A3.

Falls eine Anwendung von der TI-Plattform angebotenes Schlüsselmaterial nutzt, muss sie neben ihren eigenen Maßnahmen zum Schutz des Materials die Maßnahmen der TI-Plattform (insbesondere während der Erzeugung, Verteilung, Sperrung und Löschung) bewerten. Auch muss sie die Verwendung und die Sicherheitsmaßnahmen von anderen Anwendungen, die das betrachtete Schlüsselmaterial auch verwenden, für sich bewerten. Die Bewertung kann dann zu dem Ergebnis führen, dass das Material nicht für die Anwendung geeignet ist – die gewünscht Sicherheitsleistung kann mit diesem Material nicht erbracht werden.[3]

Um einer Anwendung Informationen über die Maßnahmen der TI-Plattform und die Nutzung in anderen Anwendungen der TI zugänglich zu machen und um nicht jede Anwendung zu zwingen den kompletten Lebenszyklus zu dokumentieren (und damit Redundanz zu vermeiden), wird für Schlüsselmaterial der TI-Plattform eine zentrale Stelle innerhalb der gematik[4] etabliert.

Anwendungen, die kryptographische Schlüssel der TI-Plattform verwenden, müssen dann nur noch ihre konkrete Nutzung des Materials anhand der vorliegenden Methode dokumentieren. Diese Dokumentation müssen sie der zentralen Stelle zur Kenntnis geben.

Es liegt im Eigeninteresse einer Anwendung, sich von der zentralen Stelle Informationen über das zur Verwendung angedachte Schlüsselmaterial einzuholen. Diese sind für die Sicherheitsanalyse der Anwendung notwendig.

[3] Beispiel Bewertung von eFA bez. der Signatur von SAML-Tokens mit dem privaten Schlüssel in PrK.HCI.OSIG.R2048 auf der SMC-B. Die Bewertung stelle die Nichteignung fest.
[4] informationssicherheit@gematik.de

3 Beispiele zur Anwendung der Methode

Die in diesem Kapitel verwendeten Beispiele haben keinen Einfluss auf die Ausgestaltung der TI.

3.1 Privater Schlüssel der eGK zur Authentifikation

Tabelle 6: Generelle Angaben

Angaben zum Schlüssel	Erläuterung
Kurzbezeichnung des Schlüsselmaterials	PrK.CH.AUT.R048
Einsatzbereich	eGK
Beschreibung des Nutzungszwecks des Schlüssels	privater Schlüssel zur Authentifikation PrK.CH.AUT.R2048
Typ des Schlüsselmaterials	privater Schlüssel eines RSA-Schlüsselpaares
Anwendung in welchem Sicherheitsverfahren	RSA (X.509v3), Authentifizierung (Entity-Authentication)
ggf. Zuordnung zu einer PKI	X.509v3-PKI unter Bridge-CA (TSL)
Maximale Gültigkeitsdauer / typische Gültig-keitsdauer	5 Jahre
Schutzbedarf	Vertraulichkeit sehr hoch Integrität hoch Authentizität hoch

Tabelle 7: Verantwortlichkeiten und Schutz

Eigenschaft	Erläuterung
Verantwortlicher	Schlüsselbesitzer ist der Versicherte (Besitzer der eGK) (Eigentümer ist der Kartenherausgeber = Krankenkasse)
Zugriffsrechte	vgl. [gemSpec_eGK_ObjSys] Abschnitt „4.5.11 MF / DF.ESIGN / PrK.CH.AUT.R2048“
Zugriffsschutz	vgl. [gemSpec_eGK_ObjSys] Abschnitt „4.5.11 MF / DF.ESIGN / PrK.CH.AUT.R2048 Sichere Schlüsselspeicher und Ausführungseinheit; Sicherheitszertifiziert nach BSI-CC-PP-0020-V3-2010-MA-01

Tabelle 8: Angaben zum Lebenszyklus

Phase	Erläuterung / Prozess	Rolle	Einsatzumgebung
Initialisierungsphase			
Erzeugung	im Trustcenter der eGK-CA oder des CMS	eGK-CA oder CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Schlüsselbackup	nein	-	-
Registrierung	im Trustcenter der eGK-CA oder des CMS	eGK-CA oder CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Erzeugung eines Schlüssel-zertifikats	im Trustcenter der eGK-CA	eGK-CA	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Verteilung	Kartenpersonalisierung und Versand der eGK an die Versicherten durch den Kartenherausgeber (Krankenkasse)	Kartenher-ausgeber (Krankenkas-se)	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter) und Erstverteilung T1 Postzustellung, Zweitverteilung T3: Postzustellung mit Ident-Prüfung
Betriebsphase			
Installation	im Trustcenter der eGK-CA oder des CMS	eGK-CA oder CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Speicherung	vgl. [gemSpec_eGK_ObjSys] Ab-schnitt „4.5.11 MF / DF.ESIGN / PrK.CH.AUT.R2048 Kartenpersonalisierung	eGK-CA oder CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Ableitung	nein	-	-
Aufheben der Registrierung / Entzug des Zertifikats	Sperrung des zugehörigen AUT-Zertifikats. über den OCSP-Responder	Kartenher-ausgeber	U13 Rechenzentrum, kontrollierter Bereich, geschützter Bereich (OCSP-Responder)
Suspendierung	zwar durch die CP theoretisch mög-lich, aber nicht vorgesehen	-	-
Reaktivierung	zwar durch die CP theoretisch mög-lich, aber nicht vorgesehen	-	-
Sperrung	Die faktische Außerbetriebnahme des privaten Signaturschlüssels der eGK nach Verwendung erfolgt durch:	a) Kartenher-ausgeber b) Inhaber	c) U13 Rechenzent-rum, kontrollierter Bereich, geschützter

Phase	Erläuterung / Prozess	Rolle	Einsatzumgebung
	a) vorzeitige Außerbetriebnahme der eGK oder, b) wiederholte falsche PIN-Eingabe oder, c) durch Sperrung des Zertifikats oder, d) durch Ablauf des Gültigkeitszeitraums des Zertifikats.	der Karte c) Kartenherausgeber d) ausführende Komponente	Bereich (OCSP-Responder)
Nach-Betriebsphase			
Archivierung	nein	-	-
Zerstörungsphase			
Löschung / Zerstörung	Die faktische Außerbetriebnahme des privaten Signaturschlüssels der eGK nach Verwendung erfolgt durch: a) vorzeitige Außerbetriebnahme der eGK oder, b) wiederholte falsche PIN-Eingabe oder, c) durch Sperrung des Zertifikats oder, d) durch Ablauf des Gültigkeitszeitraums des Zertifikats.	a) Kartenherausgeber b) Inhaber der Karte c) Kartenherausgeber d) ausführende Komponente	c) U13 Rechenzentrum, kontrollierter Bereich, geschützter Bereich (OCSP-Responder)

Umsetzung des Schutzbedarfs in den verschiedenen Einsatzumgebungen des Schlüssels:

Tabelle 9: Umsetzung Schutzbedarf des privaten Schlüssels der eGK zur Authentifikation

Vorkommen des Schlüssels	Einsatzumgebung	Umsetzung des Schutzbedarfs
Die Schlüsselerzeugung des privaten Signaturschlüssels der eGK findet im geschützten Bereich eines Sicherheitsmoduls statt, dieses befindet sich dabei im Sicherheitsbereich des Rechenzentrums des Kartenherausgebers. Der private Signaturschlüssel wird sofort nach Erzeugung im geschützten Teil eines Sicherheitsmoduls untergebracht.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Zufallserzeugung nach [TR-03116]. Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.
Ein privater Signaturschlüssel darf ein Sicherheitsmodul nicht im Klartext, sondern nur im Rahmen festgelegter Verfahren und verschlüsselt mit einem von der gematik zugelassenen kryptographischen Verfahren, verlassen.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.
Alle kryptographischen Berechnungen mit dem privaten Signaturschlüssel müssen innerhalb eines Sicherheitsmoduls erfolgen. Der Zugriff auf den privaten Signatur-	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.

Vorkommen des Schlüssels	Einsatzumgebung	Umsetzung des Schutzbedarfs
schlüssel in einem Sicherheitsmodul muss durch eine Authentifikation geschützt sein. Die Zugriffe müssen protokolliert werden, das Zugriffssystem muss durch die gematik zugelassen sein.		
Ein privater Signaturschlüssel muss in einem Sicherheitsmodul der Kartenproduktion aktiv gelöscht werden, sobald er durch dieses Sicherheitsmodul nicht mehr benötigt wird.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.
Erzeugung eines Zertifikats für den öffentlichen Signaturschlüssel der eGK passend zum privaten Signaturschlüssel der eGK, im Sicherheitsbereich des Rechenzentrums der CA. Hierbei wird der private Signaturschlüssel der eGK nicht benutzt.	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Integrität und Authentizität des öffentlichen Signaturschlüssels der eGK (und damit indirekt auch Integrität und Authentizität des privaten Signaturschlüssels der eGK) wird durch die Signatur des Zertifikats durch die CA gesichert.
Schlüsselverteilung: Der private Signaturschlüssel in der eGK wird im Zuge der Verteilung der eGK mit verteilt.	Chipkarte, geschützter Bereich U2 = U_SC_prot	Erstverteilung T1 Postzustellung, Zweitverteilung T3: Postzustellung mit Ident-Prüfung oder gleichwertige Ersatzverfahren
Schlüsselspeicherung: Der private Signaturschlüssel wird im nicht auslesbaren Teil der eGK untergebracht. Zum Signieren verlässt der Schlüssel die Karte nicht.	Chipkarte, geschützter Bereich U2 = U_SC_prot	Die Chipkarten sind dafür evaluiert den Schutzbedarf wie für den privaten Signaturschlüssel verlangt, umzusetzen
Benutzung des Schlüssels: Die Nutzung des privaten Signaturschlüssels der eGK ist mit PIN geschützt.	Chipkarte, geschützter Bereich U2 = U_SC_prot	Das PIN-Verfahren ist auf hohem Niveau durchzuführen. Besitz der eGK und Wissen der PIN gemeinsam gewährleisten die hochwertige Authentifikation.
Die faktische Außerbetriebnahme des privaten Signaturschlüssels der eGK nach Verwendung, erfolgt durch: a) vorzeitige Außerbetriebnahme der eGK oder, b) wiederholte falsche PIN-Eingabe oder, c) durch Sperrung des Zertifikats oder, d) durch Ablauf des Gültigkeitszeitraums des Zertifikats.	Chipkarte, geschützter Bereich U2 = U_SC_prot und U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.

3.2 Kartenindividueller CMS-Schlüssel

Tabelle 10: Generelle Angaben

Angaben zum Schlüssel	Erläuterung
Kurzbezeichnung des Schlüsselmaterials	SK.CMS.AES128
Einsatzbereich	eGK
Beschreibung des Nutzungszwecks des Schlüssels	Kartenindividueller Schlüssel für die gegenseitige Authentifizierung im Rahmen der Interaktion zwischen eGK und zugehörigem CMS.
Typ des Schlüsselmaterials	AES-128
Anwendung in welchem Sicherheitsverfahren	symmetrischer Schlüssel zur Authentifikation und Etablierung von Sessionkeys für MAC-Berechnung und Verschlüsselung
ggf. Zuordnung zu einer PKI	-
Maximale Gültigkeitsdauer / typische Gültigkeitsdauer	Lebensdauer einer eGK (aktuell max. 5 Jahre)
Schutzbedarf	Vertraulichkeit sehr hoch Integrität hoch Authentizität sehr hoch

Tabelle 11: Verantwortlichkeiten und Schutz

Eigenschaft	Erläuterung
Verantwortlicher	Kartenherausgeber
Zugriffsrechte	beliebiger Einsatz für Secure Messaging (SM) nach EN-14890-1
Zugriffsschutz	verlässt nach der Personalisierung das Sicherheitsmodul (eGK) nie; Anwendbar für SM immer; Liegt ebenfalls in einem Sicherheitsmodul beim CMS vor oder wird je nach Bedarf (C2S-Authentisierung / VSDD) vom CMS-master-key abgeleitet.

Tabelle 12: Angaben zum Lebenszyklus

Phase	Erläuterung / Prozess	Rolle	Einsatzumgebung
Initialisierungsphase			
Erzeugung	Bei der Kartenproduktion (Initialisierung, Personalisierung, Auslieferung) der eGK-CA: Variante A: Jede Karte ein eigener zufälliger Schlüssel, Variante B: Ableitung aus einem CMS-master-key	eGK-CA / CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Schlüsselbackup	Variante A: Jede Karte ein eigener zufälliger Schlüssel, dieser wird im CMS mit hinterlegt (Gegenstelle für die symmetri-	CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich

Phase	Erläuterung / Prozess	Rolle	Einsatzumgebung
	sche Verschlüsselung), Variante B: Ableitung aus einem CMS-master-key		(Trustcenter)
Registrierung	Variante A: Jede Karte ein eigener zufälliger Schlüssel, dieser wird im CMS mit hinterlegt (Gegenstelle für die symmetrische Verschlüsselung), Variante B: Ableitung aus einem CMS-master-key	CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Erzeugung eines Schlüssel-zertifikats	nein	-	-
Verteilung	i.d.R im CMS generiert und für die Personalisierung an die eGK-CA übergeben	eGK-CA / CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Betriebsphase			
Installation	Auf der eGK während der Personalisierung	eGK-CA / CMS	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)
Speicherung	1. in der eGK 2. zumindest temporär in eGK-CA 3. im CMS-Dienst	1.Karten hersteller 2. eGK-CA 3. CMS-Dienst	eGK: U2:Sicherheitsmodul, Chipkarte, geschützter Bereich; eGK-CA, CMS: U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich
Ableitung	es wird keine Ableitung damit durchgeführt Der Schlüssel wird für den verschlüsselten Transport von Zufallszahlen verwendet. Beide Seiten senden sich gegenseitig Zufallszahlen, diese werden mit xor verbunden und bilden den Seed für das in TR-03111 beschrieben DRBG-Verfahren. Diese liefert dann jeweils Schlüsselmaterial für die Verschlüsselung und die MAC-Bildung (Integritäts- und Authentizitätsschutz).	-	-
Aufheben der Registrierung / Entzug des Zertifikats	-	-	-
Suspendierung	-	-	-
Reaktivierung	-	-	-

Phase	Erläuterung / Prozess	Rolle	Einsatzumgebung
Sperrung	nicht vorgesehen. Bei Sperrung der Karte wird die Authentifizierung der eGK durch das CMS verweigert. Der Schlüssel wird dann nicht verwendet.	-	-
Nach-Betriebsphase			
Archivierung	-	-	-
Zerstörungsphase			
Löschung / Zerstörung	eGK: durch Vernichtung der eGK CMS: Lösung des Schlüssels bei CMS (falls kein Ableitungsverfahren mittels eines CMS-master-key verwendet wird), anderen falls Ablehnung der Schlüsselableitung für die entsprechende Karte durch das CMS-master-key-Modul	CMS	eGK: U2:Sicherheitsmodul, Chipkarte, geschützter Bereich; CMS: U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich

Tabelle 13: Notfallmaßnahmen bei Kompromittierung

Prozess	Beschreibung	Verantwortlicher
Erfassung der Kompromittierung		eGK-Besitzer / CMS
	Sperraufforderung durch den Versicherten oder durch das CMS bei Verlust der Karte oder bei bekannt werden der Kompromittierung (bspw. durch Kompromittierung des Masterkeys etc.)	
Maßnahmen zur Schadensbegrenzung im Falle der Kompromittierung		eGK-Besitzer / CMS
	eGK: durch Vernichtung der eGK CMS: Lösung des Schlüssels bei CMS (falls kein Ableitungsverfahren mittels eines CMS-master-keys verwendet wird), anderen falls Ablehnung der Schlüsselableitung für die entsprechende Karte durch das CMS-master-key-Modul	

Umsetzung des Schutzbedarfs in den verschiedenen Einsatzumgebungen des Schlüssels:

Tabelle 14: Umsetzung Schutzbedarf des kartenindividuellen CMS-Schlüssels

Vorkommen des Schlüssels	Einsatzumgebung	Maßnahmenbeschreibung
Die Schlüsselerzeugung des Master-CMS-Schlüssels der eGK findet im geschützten Bereich eines Sicherheitsmoduls statt, dieses befindet sich dabei im Sicherheitsbereich des Rechenzentrums des Kartenherausgebers. Der Master-CMS-Schlüssel wird sofort nach Erzeugung im ge-	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Zufallserzeugung nach [TR-03116]. Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.

Vorkommen des Schlüssels	Einsatzumgebung	Maßnahmenbeschreibung
schützten Teil eines Sicherheitsmoduls untergebracht.		
Ein Master-CMS-Schlüssel darf ein Sicherheitsmodul nicht im Klartext, sondern nur im Rahmen festgelegter Verfahren und verschlüsselt mit einem von der gematik zugelassenen kryptographischen Verfahren, verlassen.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.
Alle kryptographischen Berechnungen mit dem Master-CMS-Schlüssel müssen innerhalb eines Sicherheitsmoduls erfolgen. Der Zugriff auf den Master-CMS-Schlüssel in einem Sicherheitsmodul muss durch eine Authentifikation geschützt sein. Die Zugriffe müssen protokolliert werden, das Zugriffssystem muss durch die gematik zugelassen sein.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.
Schlüsselverteilung: Variante B: Der Master-CMS-Schlüssel muss nach Erzeugung dem Kartenmanagement sicher übermittelt werden. Zur Produktion der eGK muss er der Kartenproduktion sicher übermittelt werden.	Chipkarte, geschützter Bereich U2 = U_SC_prot	Erstverteilung T1 Postzustellung, Zweitverteilung T3: Postzustellung mit Ident-Prüfung oder gleichwertige Ersatzverfahren
Ein Master-CMS-Schlüssel muss in einem Sicherheitsmodul der Kartenproduktion oder des Kartenmanagements aktiv gelöscht werden, sobald er durch dieses Sicherheitsmodul nicht mehr benötigt wird.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.
Die Schlüsselerzeugung des kartenindividueller CMS-Schlüssels der eGK findet im geschützten Bereich eines Sicherheitsmoduls statt, dieses befindet sich dabei im Sicherheitsbereich des Rechenzentrums des Kartenherausgebers. Der kartenindividuelle CMS-Schlüssel wird sofort nach Erzeugung im geschützten Teil eines Sicherheitsmoduls untergebracht.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Variante A: Zufallserzeugung nach [TR-03116]. Vertraulichkeit, Integrität und Authentizität vom Rechenzentrum umzusetzen. Variante B: Zusätzlich Schutz des CMS-master-keys mit noch höheren Anforderungen. Vertraulichkeit, Integrität und Authentizität vom Rechenzentrum umzusetzen. Kritisch.
Ein kartenindividueller CMS-Schlüssel darf ein Sicherheitsmodul nicht in Klartext, sondern nur im Rahmen festgelegter Verfahren und verschlüsselt mit einem von der gematik zugelassenen kryptographischen Verfahren, verlassen.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.

Vorkommen des Schlüssels	Einsatzumgebung	Maßnahmenbeschreibung
Alle kryptographischen Berechnungen mit dem kartenindividuellen CMS-Schlüssel müssen im CMS-Dienst innerhalb eines Sicherheitsmoduls erfolgen. Der Zugriff auf den kartenindividueller CMS-Schlüssel in einem Sicherheitsmodul muss durch eine Authentifikation geschützt sein. Die Zugriffe müssen protokolliert werden, das Zugriffssystem muss durch die gematik zugelassen sein.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.
Ein kartenindividueller CMS-Schlüssel muss in einem Sicherheitsmodul der Kartenproduktion oder des Kartenmanagements aktiv gelöscht werden, sobald er durch dieses Sicherheitsmodul nicht mehr benötigt wird.	U2, U4, U6 Sicherheitsmodul, U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Sicherheitsmodul und der Umgebung (Rechenzentrum) umzusetzen.
Schlüsselverteilung: Variante A: Der kartenindividuelle CMS-Schlüssel der eGK muss von der Kartenproduktion zum Kartenmanagement sicher übermittelt werden.	U14 Rechenzentrum, kontrollierter Bereich, Sicherheitsbereich (Trustcenter)	Vertraulichkeit, Integrität und Authentizität vom Rechenzentrum umzusetzen.
Schlüsselspeicherung: Der kartenindividuelle CMS-Schlüssel der eGK wird im geschützten Teil der eGK untergebracht. Zum Authentifizieren und Aushandeln von Session-Keys verlässt der Schlüssel die Karte nicht.	Chipkarte, geschützter Bereich U2 = U_SC_prot	Die Chipkarten sind dafür evaluiert den Schutzbedarf umzusetzen
Schlüsselverteilung: Der kartenindividuelle CMS-Schlüssel in der eGK wird im Zuge der Verteilung der eGK mit verteilt.	Chipkarte, geschützter Bereich U2 = U_SC_prot	Erstverteilung T1 Postzustellung, Zweitverteilung T3: Postzustellung mit Ident-Prüfung oder gleichwertige Ersatzverfahren

Anhang A

Hinweis: Nach der Gesellschafterentscheidung, übergreifende Konzepte (wie das Kryptographiekonzept der Telematikinfrastruktur) nicht als Teil der vergaberelevanten Unterlagen zu klassifizieren, mussten Teile des Kryptographiekonzeptes hier im Anhang (insbesondere A3) untergebracht werden, damit man die hier im Dokument beschriebene Dokumentationsmethode anwenden kann.

A1 – Gültigkeitsdauer von kryptographischen Objekten

Warum ist es notwendig die Gültigkeitsdauer von kryptographischen Schlüsseln zu beschränken?

- Je länger ein Schlüssel verwendet wird, desto mehr wird mit ihm verschlüsselt, d. h. desto wertvoller wird er für einen Angreifer. Die Begehrlichkeit für einen Angreifer wächst, d.h. das Angriffspotenzial, gegen das der Schlüsselspeicher bzw. die schlüsselverarbeitenden Komponenten schützen müssen, wird immer größer. Irgendwann reicht die dem Angriffspotenzial gegenüberstehende Mechanismenstärke nicht mehr aus, da diese bestenfalls konstant bleibt (oder i. d. R. abnimmt).

- Je mehr mit einem bestimmten Schlüssel verschlüsselt wird, desto größer ist der Schaden für den Systembetreiber und den Nutzer im Fall einer Kompromittierung. Das zu tragende Risiko ist ab einem bestimmten Zeitpunkt nicht mehr tragbar. Die Begrenzung der Gültigkeitsdauer ist eine notwendige Maßnahme zur Beschränkung des Risikos.

- Je länger ein Schlüssel verwendet wird, desto größer ist die Wahrscheinlichkeit dass er durch Fehler oder Gelegenheit kompromittiert wird.

- Je mehr Kryptogramme bzw. Klartext-Chiffretext-Paare einem Angreifer zur Verfügung stehen, desto einfacher ist für ihn die Kryptanalyse. D. h. die Güte eines kryptographischen Verfahrens nimmt ab, desto länger es mit demselben Schlüssel aktiv verwendet wird. Dieser Effekt ist unabhängig von der natürlichen Schwächung der Algorithmen durch unaufhaltbare Fortschritte bei „Wissenschaft und Technik“. Das Verfahren kann seinen Bestimmungszweck ab einem bestimmten Zeitpunkt nicht mehr erfüllen, weil die Mechanismenstärke zu sehr gesunken ist.

- Durch die Limitierung der Gültigkeitsdauer wird auch die Zeit limitiert, die einem Angreifer für rechenintensive Kryptoanalysen und für die physikalische Überwindung von Sicherungsmaßnahmen für das zu schützende Schlüsselmaterial zur Verfügung steht. Ziel ist es, dass zu dem Zeitpunkt zu dem die Schlüssel extrahiert werden können, diese nicht mehr gültig sind. Dann wären alte Kryptogramme zwar dechiffrierbar, aber die Schlüssel wären nicht mehr aktiv durch Angreifer verwendbar, da sie von Systemkomponenten als ungültige Schlüssel abgelehnt werden würden.

- Die Limitierung der Gültigkeitsdauer sorgt dafür, dass ein kryptographischer Algorithmus auch ohne organisatorischen Eingriff nicht länger verwendet werden wird, als dessen voraussichtliche effektive Lebenszeit.
- Durch das regelmäßige und nicht zu seltene Üben des Schlüsselwechsels werden die notwendigen Maßnahmen trainiert bzw. aufrechterhalten (Wechsel von Mitarbeitern, geänderte Umgebungsbedingungen (die erst beim Training auffallen), anpassen von Vertragsbedingungen etc.).

A2 – Typen von Einsatzumgebungen und Transportarten

Die folgende Tabelle definiert die Typen von Einsatzumgebungen und Transportarten.

Tabelle 15: Typen von Einsatzumgebungen

Nr.	Kürzel	Umgebungstyp	Realisierung	Schutz
U1	U_SC (SC = Smartcard)	Sicherheitsmodul	Chipkarte	allgemeiner Bereich
U2	U_SC_prot	Sicherheitsmodul	Chipkarte	geschützter Bereich
U3	U_TPM	Sicherheitsmodul	TPM	allgemeiner Bereich
U4	U_TPM_prot	Sicherheitsmodul	TPM	geschützter Bereich
U5	U_HSMg	Sicherheitsmodul	HSM	allgemeiner Bereich
U6	U_HSM_prot	Sicherheitsmodul	HSM	geschützter Bereich
U7	U_OP_pub (OP= operating Env.)	Büro/Praxis/Apotheke/Station	Zugänglicher Bereich	Gerät geschlossen/ ohne Aufsicht
U8	U_OP_SV (SV = Supervision)	Büro/Praxis/Apotheke/Station	Bereich unter Aufsicht	unter Aufsicht oder einfacher Zugangskontrolle
U9	U_OP_PC (PC = Permanent Control)	Büro/Praxis/Apotheke/Station	Zugänglicher Bereich	unter ständiger Kontrolle
U10	U_OP_batchsig	Büro/Praxis/Apotheke/Station	Besonders gesicherte Umgebung für Stapelsignatur	HBA unter Verschluss
U11	U_Home	Home	nicht zugänglicher Bereich	Raum unter Verschluss, persönliche Verantwortung
U12	U_DC (DC = data center)	Rechenzentrum	allgemeiner Bereich	
U13	U_DC_Prot	Rechenzentrum	kontrollierter Bereich	geschützter Bereich
U14	U_DC_Sec	Rechenzentrum	kontrollierter Bereich	Sicherheitsbereich

Tabelle 16: Sicherheitsstufen physikalische Sicherheit der Geräte

Nr.	Kürzel	Schutz
G0	closed	Gerät verschlossen
G1	TE (Tamper-evident)	Gerät verschlossen, Angriffe erkennbar
G2	TD (Tamper detection)	Gerät verschlossen, Angriff wird erkannt und gemeldet
G2	TR (Tamper Resistance)	Gerät verschlossen, Autom. Schutz gegen Angriffe

Tabelle 17: Arten des Transports von Schlüsselmaterial

Nr.	Umgebungstyp	Realisierung	Schutz
T1	Postweg	allgemeiner Postversand	
T2		kontrollierter Postversand	Einschreiben
T3		kontrollierter Postversand	Post-Identverfahren
T4	Werttransport	besondere Bestimmungen für die betrauten Personen	Sicherheitsumgebungen
T5	elektronischer Transport	öffentliches Netz	Payload verschlüsselt
T6		öffentliches Netz	Alles verschlüsselt
T7		nicht öffentlich zugängliches Netz	Unverschlüsselt
T8		nicht öffentlich zugängliches Netz	Payload verschlüsselt
T9		nicht öffentlich zugängliches Netz	Alles verschlüsselt
T10		gesichertes Netz	Unverschlüsselt
T11		gesichertes Netz	Payload verschlüsselt
T12		gesichertes Netz	Alles verschlüsselt

A3 – Die einzelnen Phasen des Lebenszyklus von kryptographischen Schlüsseln

Der komplette Lebenszyklus eines Schlüssels muss vom Erzeuger (meint hier Spezifikateur) festgelegt werden, Maßnahmen zu seinem Schutz müssen spezifiziert werden. In Abbildung 2 sind die Zustände im Lebenszyklus eines Schlüssels dargestellt:

- **Noch nicht aktiv:** Der Schlüssel ist erzeugt, aber noch nicht aktiviert.
- **Aktiv:** In der Betriebsphase wird der Schlüssel gebraucht, um Information kryptographisch zu bearbeiten.
- **Post aktiv:** Der Schlüssel darf nicht mehr für kryptographische Aktivitäten verwendet werden. Der Grad der Suspendierung muss genau beschrieben werden, wie auch die Umstände, unter denen der Schlüssel ggf. wieder aktiviert werden kann.

- **Zerstört (Endgültig gesperrt):** Ein endgültig gesperrter Schlüssel darf nicht mehr verwendet werden. Ein endgültig gesperrter Schlüssel soll sicher in allen Komponenten zerstört werden. Dies kann auch durch organisatorische Maßnahmen (z. B. Einziehen von Karten) geschehen.

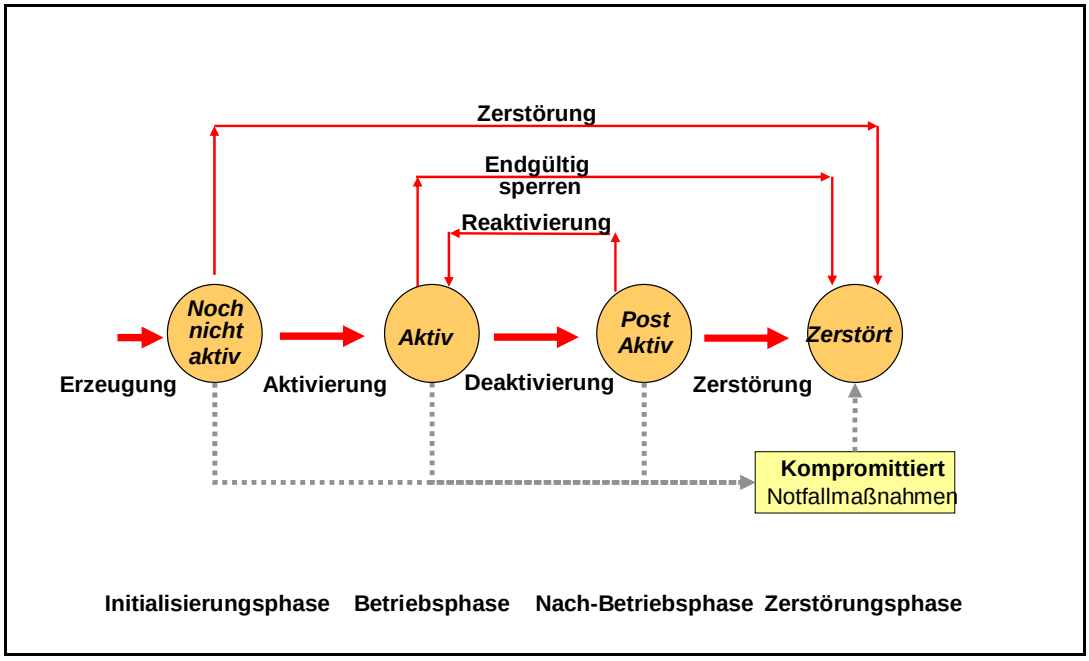

Abbildung 2: Lebenszyklus der Schlüssel und die Übergänge zwischen den Zuständen eines Schlüssels

In Abbildung 2 sind die Übergänge zwischen den Zuständen eines Schlüssels dargestellt

- **Erzeugung** ist der Prozess, einen Schlüssel zu erzeugen. Der Schlüssel muss dabei nach bestimmten Vorgaben erzeugt werden. Soweit wie möglich soll der Prozess Tests enthalten, die die Einhaltung der Vorgaben überprüfen.
- **Aktivierung,** dieser Prozess macht einen Schlüssel gültig. Der Schlüssel darf in kryptographischen Operationen nicht zu anderen Zwecken als zu seinem Verwendungszweck eingesetzt werden.
- **Deaktivierung,** dieser Prozess schränkt den Gebrauch eines Schlüssels ein. Der Schlüssel darf nicht mehr für kryptographische Operationen verwendet werden. Dies muss geschehen, wenn die Gültigkeit des Schlüssels ausgelaufen ist oder weil der Schlüssel aufgrund eines Ereignisses suspendiert und gesperrt wurde.
- **Reaktivierung,** dieser Prozess macht einen Schlüssel wieder gültig. Der Schlüssel kann nun wieder in den für diesen Schlüssel erlaubten kryptographischen Operationen eingesetzt werden.
- **Zerstörung** beendet den Lebenszyklus des Schlüssels. Das beinhaltet die logische endgültige Sperrung und die physikalische Zerstörung des Schlüssels.
- **Kompromittiert:** In jeder Phase kann ein Schlüssel kompromittiert werden. Die für diesen Fall definierten Notfallmaßnahmen sind einzuleiten – z. B. die betrof-

fenen Karten sperren und die Karten tauschen. Nach der Durchführung der Notfallmaßnahmen ist der Schlüssel zu zerstören.

Die betrachteten Übergänge beinhalten eine Anzahl von Schlüsselmanagementdiensten.

- **KMS 1. Schlüsselerzeugung:** Schlüsselerzeugung ist ein Dienst, der aufgerufen wird, um auf sicherem Wege Schlüssel für einen bestimmten kryptographischen Algorithmus zu erzeugen. Dies erfordert, dass die Schlüsselerzeugung nicht manipulierbar sein darf, die Schlüssel nicht vorhersagbar sein dürfen und in der vorgeschriebenen statistischen Verteilung erzeugt werden müssen.
  Diese statistischen Verteilungen sind vom verwendeten kryptographischen Schlüssel und vom geforderten Niveau des kryptographischen Schutzes erzwungen.
  Die Erzeugung mancher Schlüssel, z. B. Master-Keys, erfordert besondere Sorgfalt und besonderen Schutz, da die Kenntnis dieser Schlüssel Zugriff auf die verbundenen oder abgeleiteten Schlüssel ermöglicht. Für die Erzeugung der Schlüssel des Versicherten sollen bauliche, personelle und organisatorische Maßnahmen äquivalent zu einem Zertifizierungsdienst gemäß [SigG01] eingehalten werden.

- **KMS 2. Schlüsselregistrierung:** Der Dienst Schlüsselregistrierung verbindet einen Schlüssel mit einer Entität.
  Er wird von einer Registrierungsinstanz angeboten und üblicherweise angewandt, wenn symmetrische Kryptographie benutzt wird. Wenn eine Entität einen Schlüssel registrieren lassen will, kontaktiert sie die Registrierungsinstanz. Schlüsselregistrierung beinhaltet eine Registrierungsanforderung und eine Bestätigung dieser Registrierung. Eine Registrierungsinstanz pflegt ein Register von Schlüsseln und die dazugehörigen Informationen in hinreichend sicherer Art und Weise.

- **KMS 3. Erzeugung eines Schlüsselzertifikats:** Der Dienst „Erzeugung eines Schlüsselzertifikats“ verbindet einen öffentlichen Schlüssel mit einer Entität und wird von einer Zertifizierungsinstanz betrieben. Wenn eine Anforderung zur Schlüsselzertifizierung akzeptiert wird, erzeugt die Zertifizierungsinstanz ein Schlüsselzertifikat.

- **KMS 4. Schlüsselverteilung:** Die Schlüsselverteilung ist eine Menge von Prozessen, um Schlüsselmanagementinformationsobjekte (in der Regel Schlüssel) sicher zu autorisierten Entitäten zu verteilen.

- **KMS 5. Schlüsselinstallation:** Der Dienst Schlüsselinstallation ist immer vor dem Gebrauch eines Schlüssels notwendig. Bei der Schlüsselinstallation wird der Schlüssel in einer Art und Weise eingebracht, die den Schlüssel vor Kompromittierung schützt.

- **KMS 6. Schlüsselspeicherung:** Der Dienst Schlüsselspeicherung bietet sichere Speicherung für Schlüssel im laufenden oder zukünftigen Gebrauch oder auch für Backup-Schlüssel. Es ist üblicherweise von Vorteil, physikalisch getrennte Schlüsselspeicher vorzusehen. Zum Beispiel sichert ein Schlüsselspeicher die Vertraulichkeit und Integrität von Schlüsselmaterial oder die Integrität von öffentlichen Schlüsseln. Speicherung kann in allen Schlüsselzuständen im Lebenszyklus eines Schlüssels vorkommen.

- **KMS 7. Schlüsselableitung:** Der Dienst Schlüsselableitung erstellt eine potentiell große Anzahl von Schlüsseln unter Benutzung eines geheimen Originalschlüssels, genannt Ableitungsschlüssel, nicht geheimen veränderlichen Daten und mit einem Transformationsprozess (der nicht immer geheim sein muss). Das Ergebnis dieses Prozesses ist der abgeleitete Schlüssel. Der Ableitungsschlüssel erfordert besonderen Schutz. Der Ableitungsprozess muss unumkehrbar und nicht-vorhersehbar sein um sicherzustellen, dass die Kompromittierung eines abgeleiteten Schlüssels nicht den Ableitungsschlüssel oder andere abgeleitete Schlüssel kompromittiert.

- **KMS 8. Schlüsselarchivierung:** Schlüsselarchivierung ist der Prozess, Schlüssel nach Ablauf der Nutzung sicher und langfristig zu speichern. Für diesen Dienst ist die Anwendung des Dienstes “Schlüsselspeicherung” denkbar, es bestehen aber verschiedene Anforderungen, so dass auch verschiedene Implementierungen denkbar sind. So könnte z. B. die Schlüsselarchivierung offline realisiert werden. Archivierte Schlüssel können noch lange nach dem normalen Gebrauch der Schlüssel benötigt werden, um bestimmte Ansprüche abzuklären

- **KMS 9. Schlüsselsuspendierung:** Wenn die Kompromittierung eines Schlüssels bekannt ist oder vermutet wird, stellt der Dienst Schlüsselsuspendierung die sichere Deaktivierung des Schlüssels sicher. Der Dienst ist auch für Schlüssel, deren Gültigkeit abgelaufen ist, notwendig. Schlüsselsuspendierung wird auch dann angewandt, wenn sich die Rahmenbedingungen beim Schlüsselinhaber ändern. Nach der Suspendierung kann der Schlüssel nur eingeschränkt benutzt werden (In der Regel nicht mehr um zu verschlüsseln oder zu signieren, aber der Schlüssel darf gebraucht werden um zu entschlüsseln oder zu verifizieren). Der Grad der Suspendierung muss genau beschrieben werden, wie auch die Umstände, unter denen der Schlüssel wieder aktiviert werden kann.

  Der Dienst Schlüsselsuspendierung wird kaum bei zertifikatsbasierten Schemata angewandt, wo der Lebenszyklus der Schlüssel durch die Gültigkeit der Zertifikate geregelt wird.

- **KMS 10. Aufheben der Registrierung eines Schlüssels:** Der Dienst Aufheben der Registrierung eines Schlüssels wird von einer Registrierungsinstanz angeboten, die die Verbindung des Schlüssels mit einer Entität aufhebt. Er ist Teil des Schlüsselzerstörungsprozesses. Wenn eine Entität die Registrierung eines Schlüssels aufheben lassen will, kontaktiert sie die Registrierungsinstanz.

- **KMS11. Schlüsselzerstörung:** Der Dienst Schlüsselzerstörung bietet einen Prozess für die sichere Zerstörung von Schlüsseln an, die nicht mehr gebraucht werden. Zerstörung eines Schlüssels bedeutet, alle Einträge des Schlüsselmanagementinformationsobjekts zu löschen, so dass nach der Zerstörung keine Information übrig bleibt, um den zerstörten Schlüssel wiederherzustellen. Dies wird gemacht, um die Zerstörung alle archivierten Kopien sicherzustellen. Dennoch, bevor archivierte Schlüssel zerstört werden, sollte eine Prüfung gemacht werden um sicherzustellen, dass kein Material, das durch diese Schlüssel geschützt wird, jemals wieder gebraucht wird.

NOTIZ: Es können Schlüssel außerhalb von elektronischen Geräten oder Systemen gespeichert sein (bspw. ausgedruckt als 2D-Barcode und aufbewahrt in einem Tresor). Das erfordert zusätzliche administrative Maßnahmen.

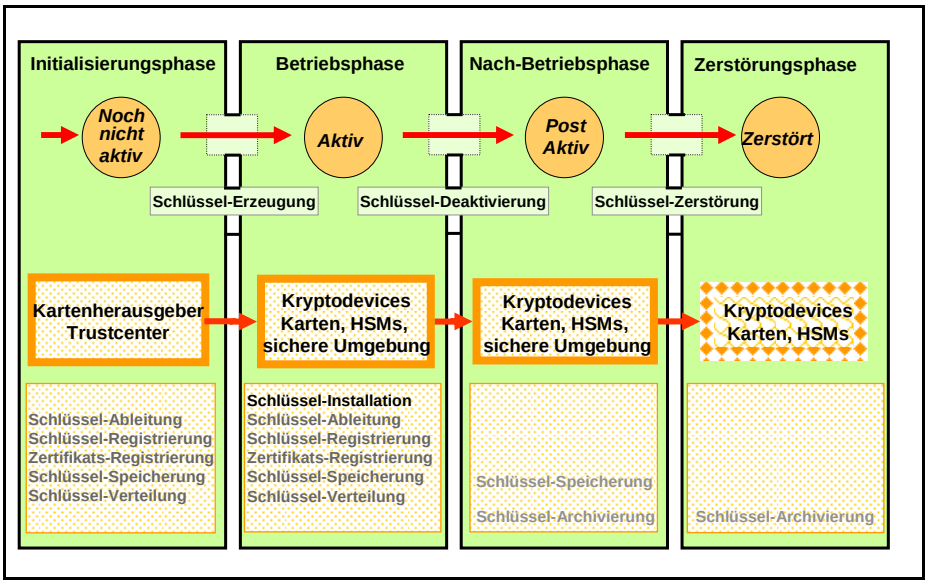

Abbildung 3: Betriebsphasen im Schlüssellebenszyklus und Keymanagement-Dienste nach [ISO11770]

In der folgenden Tabelle sind die verschiedenen Phasen des Lebenszyklus und ihre Realisierung durch einen Schlüsselverwaltungsdienst benannt.

Tabelle 18: Übergänge zwischen den Zuständen eines Schlüssels, realisiert durch Schlüsselmanagementdienste (siehe [ISO11770])

Übergang	Schlüsselmanagementdienste	Bemerkungen
Erzeugung	Schlüsselerzeugung	obligatorisch
	Schlüsselregistrierung	optional, entweder hier oder bei der Aktivierung
	Erzeugung eines Schlüsselzertifikats	optional
	Schlüsselverteilung	optional
	Schlüsselspeicherung	optional
Aktivierung	Erzeugung eines Schlüsselzertifikats	optional
	Schlüsselverteilung	optional
	Schlüsselableitung	optional
	Schlüsselinstallation	obligatorisch
	Schlüsselspeicherung	optional
	Registrierung eines Schlüssels	optional, entweder hier oder bei der Erzeugung
Deaktivierung	Schlüsselspeicherung	optional

Übergang	Schlüsselmanagementdienste	Bemerkungen
	Schlüsselarchivierung	optional, entweder hier oder bei der Zerstörung
	Schlüsselsuspendierung	obligatorisch
Reaktivierung	Erzeugung eines Schlüsselzertifikats	optional
	Schlüsselverteilung	optional
	Schlüsselableitung	optional
	Schlüsselinstallation	obligatorisch
	Schlüsselspeicherung	optional
Zerstörung	Schlüsselderegistrierung	obligatorisch; wenn registriert
	Schlüsselzerstörung	obligatorisch
	Schlüsselarchivierung	optional, entweder hier oder bei der Deaktivierung
Endgültig Sperren	Schlüsselsuspendierung	obligatorisch
	Schlüsselderegistrierung	obligatorisch; wenn registriert
	Schlüsselzerstörung	obligatorisch

A4 – Glossar

Das Glossar wird als eigenständiges Dokument [gemGlossar] zur Verfügung gestellt.

A5 – Abbildungsverzeichnis

A6 – Tabellenverzeichnis

A7 - Referenzierte Dokumente

A7.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar
[gemSpec_eGK_ObjSys]	gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem

A7.2 – Weitere Dokumente

[Quelle]	Herausgeber, Titel, Erscheinungsdatum etc.
[Kerck-1883]	Auguste Kerckhoffs, "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, Seite 5–83, Jan. 1883, Seite 161–191, Feb. 1883. siehe auch http://www.petitcolas.net/fabien/kerckhoffs/ (Link geprüft: 26.05.2011)
[ISO-11770]	ISO/IEC 11770: 1996 Information technology - Security techniques - Key management Part 3: Mechanisms using asymmetric techniques
[SigG01]	Bundesgesetzblatt I (2001), S.876: Signaturgesetz vom 16. Mai 2001 (BGBl.I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)
[TR-03116]	BSI TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version: 3.16, Datum: 07.08.2012 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116_pdf.html (Link geprüft: 09.10.2012)