Einführung der Gesundheitskarte

Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur

Version:	1.1.0
Revision:	\main\rel_online\rel_ors1\7
Stand:	21.02.2014
Status:	freigegeben
Klassifikation:	öffentlich
Referenzierung:	[gemSpec_PINPUK_TI]

Dokumentinformationen

Änderungen zur Vorversion

Losübergreifende Synchronisation

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	22.02.12		Ableitung des Dokumentes aus [gemSiko#AnhE]	ITS/SI
	24.02.12		Redaktionelle Überarbeitung im Rahmen des Projektes Online-Rollout Stufe 1, insbesondere die Umnummerierung der Anforderungsnummern entsprechend der Vorgaben des Projektes. Ergänzen des Anhangs A (Eingangsanforderungen) und Anhangs B (Ausgangsanforderungen)	ITS/SI
0.9.0	27.02.12		formale QS	QM
0.9.1	20.04.12	Kap. 2.1, Kap. 4	Ergänzung Kapitel 2.1 und Einführung von Kapitel 4.	ITS/SI
0.10.0	20.04.12		zur Abstimmung freigegeben	gematik
			Anpassung an die Inhalte und Struktur der vergaberelevanten Dokumente	ITS/SI
0.15.0	11.01.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Gesellschafterkommentare	P77
0.19.0	22.04.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare LA	P77
1.0.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.0.0	06.06.13		freigegeben	gematik
			Losübergreifende Synchronisation	P77
1.1.0	21.02.14		freigegeben	gematik

© gematik - öffentlich

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einordnung des Dokumentes 4

1.1 Zielsetzung 4

1.2 Zielgruppe 4

1.3 Geltungsbereich 4

1.4 Abgrenzung 5

1.5 Methodik 5

2 Mindestanforderungen und Sicherheits-Policies für die Behandlung von PIN/PUK 6

2.1 PIN/PUK-Erzeugung 7

2.2 PIN/PUK-Speicherung 9

2.3 PIN/PUK-Transport 11

2.4 PIN/PUK-Verwendung 13

2.5 PIN -Änderung 13

2.6 PIN/PUK-Löschung 14

3 Mindestanforderungen und Sicherheits-Policies für die Behandlung der Schlüssel zum Schutz der PIN/PUK 16

Anhang A - Verzeichnisse 17

A1 - Abkürzungen 17

A2 - Glossar 17

A3 - Referenzierte Dokumente 17

A3.1 – Dokumente der gematik 17

A3.2 – Weitere Dokumente 18

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die übergreifende PIN/PUK-Policy für Smartcards der TI gilt für den Gesamtbereich Kartenproduktion, Kartenausgabe, Karteneinzug der eGK[1] und der HBA[2]/SMC sowie für die Verwendung von deren PINs und den zugehörigen PUKs an allen betroffenen Komponenten der Telematikinfrastruktur.

Die Anforderungen der übergreifenden PIN/PUK-Policy für Smartcards der TI stellen sicher, dass die PINs und zugehörige PUKs in der TI in jedem Verarbeitungsschritt und zu jedem Zeitpunkt auf einem einheitlichen Mindestniveau geschützt werden. Dadurch werden auch die Daten der TI auf einem adäquaten Sicherheitsniveau geschützt, auf die nach erfolgreicher Eingabe der PIN/PUK zugegriffen werden kann.

Durch die übergreifende PIN/PUK-Policy für Smartcards der TI wird auch sichergestellt, dass die PIN/PUK für in der TI hinzukommende Smartcards mit einem einheitlichen Mindestniveau geschützt werden.

1.2 Zielgruppe

Das Dokument richtet sich an Kartenherausgeber von eGK und HBA/SMC. Kartenherausgeber können Dritte mit der Kartenpersonalisierung beauftragen. In diesem Fall, in dem der Kartenherausgeber operative Aufgaben durch einen Dritten wahrnehmen lässt, muss der beauftragte Auftragnehmer die Anforderungen einhalten. Es bleibt jedoch in der Verantwortung des Kartenherausgebers sicherzustellen, dass der Beauftragte die Anforderungen umsetzt. Bei der Auswahl des Auftragnehmers ist hierauf zu achten.

Falls ein Trust Service Provider (TSP) ein akkreditierter Zertifizierungsdiensteanbieter nach Signaturgesetz (SigG) ist und das Sicherheitskonzept nach § 4 Abs. 2 SigG auch die Verarbeitung der Informationsobjekte der TI abdeckt, kann der TSP die Einhaltung der Datenschutz- und Sicherheitsanforderungen der gematik durch ein gültiges Gütezeichen nachweisen, dass er von der nach SigG zuständigen Behörde erhalten hat.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren

[1] Falls die eGK eine qualifizierte elektronische Signatur besitzt, so wird die PIN für diese qualifizierte elektronische Signatur von der BNetzA geregelt und ist nicht Gegenstand dieses Dokumentes.

[2] Die PINs für die qualifizierte elektronische Signatur eines HBA werden von der BNetzA geregelt und sind nicht Gegenstand dieses Dokumentes.

Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Wichtiger Schutzrechts-/Patentrechtshinweis:

Das vorliegende Sicherheitskonzept ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik übernimmt insofern keinerlei Gewährleistungen

1.4 Abgrenzung

Das Dokument definiert Anforderungen an Produkte und Verfahren, stellt jedoch keine Lösungsbeschreibungen dar.

1.5 Methodik

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem RFC 2119 [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte (MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN) verwendet.

Sie werden im Dokument wie folgt dargestellt:

⌦ **GS-A_xxxx <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Mindestanforderungen und Sicherheits-Policies für die Behandlung von PIN/PUK

Der Zugriff auf personenbezogene und medizinische Daten der Telematikinfrastruktur (TI) ist unter anderem durch kryptographische Schlüssel geschützt, die auf Smartcards gespeichert sind und durch die Eingabe von PINs freigeschaltet werden. Um die Daten der TI auf einem adäquaten Sicherheitsniveau zu schützen, sind daher auch diese PINs der Smartcards in der TI in jedem Verarbeitungsschritt und zu jedem Zeitpunkt auf einem einheitlichen Mindestniveau zu schützen. Diese Mindestanforderungen gelten in gleicher Weise für PUKs, die für PIN-Änderungen bzw. für das Zurücksetzen des Fehlbedienungszählers einer PIN benötigt werden. Die Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, die Kartenpersonalisierer müssen bei der Auslieferung der Karten auch für die geschützte Übermittlung der benötigten PINs und PUKs sorgen.

Dieses Kapitel beschreibt die Mindestanforderungen an die Behandlung von PIN/PUK, damit unabhängig von der jeweils gewählten Verfahrensvariante zur Aushändigung der PIN/PUK-Briefe und der Karten (z.B. Transport-PIN-Verfahren oder Echt-PIN-Verfahren) ein einheitliches Sicherheitsniveau für die PIN/PUK in der Telematikinfrastruktur gewährleistet werden kann.

⌦ **GS-A_2229 Prozesse und Maßnahmen zur Aushändigung von Karte und PIN/PUK-Brief**

Die Erreichung der Schutzziele Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und Nichtabstreitbarkeit sowie die Wirksamkeit und Konsistenz der gewählten Maßnahmen und Prozesse zur Aushändigung der PIN/PUK-Briefe sowie der Karten MUSS vom Kartenherausgeber bewertet und gewährleistet werden.⌫

Es ist vorgesehen, dass der Karteninhaber seinen persönlichen Willen durch Besitz (der Karte) und Wissen (der PIN) ausdrücken kann. Mit diesen PINs zur Authentifizierung werden kryptographische Schlüssel zugänglich, die einen Zugriff auf personenbezogene und medizinische Daten ermöglichen. Daraus resultieren u. A. die Anforderungen:

⌦ **GS-A_2227 Keine Kartendubletten**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS technisch kontrollieren und zusichern, dass jede Karte mit der zugehörigen PIN/PUK nur einmal existiert (keine Kartendubletten) und auch nur einmal an den Karteninhaber sicher ausgegeben wird.⌫

⌦ **GS-A_2228 Trennung von Karte und PIN/PUK-Brief**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS organisatorisch sicherstellen, dass Karte und PIN/PUK-Brief bis zur Übergabe an den Karteninhaber nie gemeinsam an einer Stelle beim Kartenherausgeber bzw. Kartenpersonalisierer vorhanden sind, z. B. durch den getrennten Versand mit einem Mindestabstand von drei Tagen mit unterschiedlichen Rücksendeadressen.⌫

In den nachfolgenden Unterkapiteln werden die für HBA, SMC und eGK mindest einzuhaltenden Sicherheitsanforderungen und –policies über den gesamten Lebenszyklus beschrieben. Es werden dabei die folgenden Phasen unterschieden:

- PIN/PUK-Erzeugung
- PIN/PUK-Speicherung
- PIN/PUK-Transport
- PIN/PUK-Verwendung
- PIN/PUK-Änderung
- PIN/PUK-Löschung

2.1 PIN/PUK-Erzeugung

Grundsätzlich sind für die PIN-Erzeugung Verfahren möglich, bei denen die Auswahl einer PIN durch den Karteninhaber erfolgt oder bei dem die PIN dem Karteninhaber durch den Kartenherausgeber bzw. Kartenpersonalisierer zugewiesen wird.

⌦ **GS-A_2232 PIN/PUK-Erzeugung: Verfahren für PIN/PUK-Auswahl**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die PIN/PUK-Auswahl gemäß einer der folgenden Techniken erfolgt:

- zugewiesene zufällige oder pseudozufällige PIN/PUK
- zugewiesene abgeleitete PIN/PUK
- durch Karteninhaber gewählte PIN.

Festlegungen in den Spezifikationen eines Kartentyps können die erlaubten Verfahren weiter einschränken. ⌫

⌦ **GS-A_2239 PIN/PUK-Erzeugung: Ableitung von PIN im Sicherheitsmodul**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS die PIN/PUK in einem Sicherheitsmodul mit geprüften Algorithmen gemäß der Mindeststandards der gematik entsprechend [gemSpec_Krypt] erzeugen oder ableiten, so dass sie nicht von Unbefugten ausgelesen oder manipuliert werden können.⌫

Die Mindestanforderungen der gematik an kryptographische Algorithmen sind in [gemSpec_Krypt] beschrieben.

Falls der Kartenherausgeber bzw. der Kartenpersonalisierer die PINs zuweist, so können die PINs/PUKs entweder (pseudo-)zufällig erzeugt oder aus Kartendaten abgeleitet werden.

⌦ GS-A_2234 PIN/PUK-Erzeugung: Zufallsgenerator für PIN/PUK

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass, falls die PIN/PUK zufällig oder pseudozufällig erzeugt wird, der dabei verwendete Zufalls- oder Pseudozufallsgenerator die vorgegebenen Mindestanforderungen der gematik entsprechend [gemSpec_Krypt] erfüllt. ⌫

Die Mindestanforderungen der gematik an einen Zufalls- oder Pseudozufallsgenerator sind in [gemSpec_Krypt] beschrieben.

⌦ GS-A_2235 PIN/PUK-Erzeugung: Ableitung von PIN

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass, falls die PIN/PUK aus Kartendaten abgeleitet wird, die abgeleitete PIN/PUK ohne Kenntnis des benutzten Schlüssels nicht einfacher bestimmt werden kann als eine zufällig erzeugte PIN/PUK.⌫

Der Kartenherausgeber bzw. Kartenpersonalisierer muss bei der Ableitung der PIN also insbesondere verhindern, dass der Ableitungsprozess spezielle Werte bevorzugt erzeugt und dass zugewiesene PIN/PUK gleich verteilt sind, um das Erraten einer PIN/PUK zu erschweren.

⌦ GS-A_2236 PIN/PUK-Erzeugung: Ableitung der PIN aus eindeutig dem Versicherten zugeordneten Daten

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass, falls die PIN/PUK aus Kartendaten abgeleitet wird, sie kryptographisch von vollständigen Kartenidentifikationsdaten, die eineindeutig dem Versicherten zugeordnet sind, abgeleitet wird. ⌫

⌦ GS-A_2237 PIN/PUK-Erzeugung: kein Rückschluss von PIN/PUK auf Schlüssel

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass, falls die PIN/PUK aus Kartendaten abgeleitet wird, aus der Kenntnis der PIN/PUK und der Inputdaten keine Informationen über den benutzten Schlüssel des Kartenherausgebers bzw. Kartenpersonalisierers abgeleitet werden können. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS sicherstellen, dass die Mindestanforderungen der gematik für die kryptographischen Algorithmen entsprechend [gemSpec_Krypt] erfüllt werden. ⌫

Die Mindestanforderungen der gematik an kryptographische Algorithmen sind in [gemSpec_Krypt] beschrieben.

Falls die PIN vom Karteninhaber gewählt wird, ist dieser über die Anforderungen an die PIN-Auswahl zu informieren.

⌦ GS-A_2230 PIN/PUK-Erzeugung: Länge PIN/PUK (Kartenherausgeber)

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS den Karteninhaber

bei einer durch den Karteninhaber selbst zu wählenden PIN, über die Länge der PIN informieren. ⌫

⌦ **GS-A_2238 PIN/PUK-Erzeugung: Informationen an Karteninhaber bei selbstständiger Wahl der PIN**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS, falls die PIN durch die Karteninhaber gewählt wird, dem Karteninhaber entsprechende Auswahlanweisungen sowie Warnungen geben und dem Karteninhaber bei der Kartenausgabe zusenden.⌫

2.2 PIN/PUK-Speicherung

Eine Speicherung von PINs/PUKs beim Herausgeber für die Nutzung im Produktionsprozess erfolgt nur so lange, bis PIN und PUK auf die Karte und den PIN/PUK-Brief übertragen wurden.

⌦ **GS-A_5209 PIN/PUK-Speicherung: PIN/PUK unverzüglich löschen**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS die PIN/PUK einer Karte in seinen Systemen unverzüglich löschen, nachdem PIN und PUK auf die Karte übertragen und der PIN/PUK-Brief an den Karteninhaber erstellt wurden.⌫

Die gespeicherte PIN darf nicht abgehört oder unbemerkt manipuliert werden können. PINs dürfen nur innerhalb von Sicherheitsmodulen (Chip, HSM) und Sicherheitsobjekten (inkl. PIN/PUK-Briefe) im Klartext vorliegen.

⌦ **GS-A_2240 PIN/PUK-Speicherung: Verschlüsselung der PIN außerhalb von Sicherheitsmodulen**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS die PIN/PUK verschlüsseln, falls die PIN/PUK außerhalb eines Sicherheitsmoduls gespeichert wird. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS sicherstellen, dass die dabei verwendeten kryptographischen Algorithmen die aktuellen Mindestanforderungen der gematik entsprechend [gemSpec_Krypt] erfüllen.⌫

⌦ **GS-A_2242 PIN/PUK-Speicherung: Integrität der PIN außerhalb von Sicherheitsmodulen**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS die Integrität der PIN/PUK schützen, falls die PIN/PUK außerhalb eines Sicherheitsmoduls gespeichert wird. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS sicherstellen, dass die dabei verwendeten kryptographischen Algorithmen die aktuellen Mindestanforderungen der gematik entsprechend [gemSpec_Krypt] erfüllen.⌫

Die Mindestanforderungen der gematik an kryptographische Algorithmen sind in [gemSpec_Krypt] beschrieben.

GS-A_2244 PIN/PUK-Speicherung: Verschlüsselung unterschiedlicher PINs mit unterschiedlichen Schlüsseln

Falls PINs bzw. PUKs außerhalb der Karte gespeichert werden, dann MUSS der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer für den Schutz unterschiedlicher PINs und der PUK einer Karte während der Speicherung verschiedene Verschlüsselungsschlüssel verwenden.

GS-A_2246 PIN/PUK-Speicherung: Verschlüsselung gleicher PINs führt zu unterschiedlichen verschlüsselten Werten

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass falls zwei PINs zufällig den gleichen Wert aufweisen, diese bei der Verschlüsselung zur Speicherung beim Kartenherausgeber bzw. Kartenpersonalisierer nicht auf den gleichen verschlüsselten Wert abgebildet werden.

GS-A_2247 PIN/PUK-Speicherung: Wiederholte Verschlüsselung der PIN führt zu unterschiedlichen Werten

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass, falls dieselbe PIN wiederholt verschlüsselt wird, die entsprechenden verschlüsselten Werte unterschiedlich sind.

GS-A_2248 PIN/PUK-Speicherung: unterschiedliche Schlüssel für unterschiedliche Zwecke

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass für das Verschlüsseln der PIN zur Speicherung je Verwendungszweck bzw. Empfänger (u. a. PIN-Druck, Chip-Personalisierung, Speicherung) unterschiedliche Schlüssel verwendet werden.

GS-A_2249 PIN/PUK-Speicherung: Dokumentation der Zwecke

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass für die Schlüssel die entsprechenden Verwendungszwecke bzw. Empfänger dokumentiert werden.

Die Dokumentation dient zum Nachweis der korrekten Schlüsselverwendung und kann u.a. im Falle von Audits herangezogen werden.

GS-A_2250 PIN/PUK-Speicherung: Entschlüsselung nur durch berechtigten Empfänger

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS durch geeignete organisatorische und technische Maßnahmen (z. B. Schlüsseltrennung, getrennte HSMs) sicherstellen, dass nur innerhalb der Sicherheitsmodule berechtigter Empfänger und Komponenten die PIN entschlüsselt und im Klartext vorliegen kann.

2.3 PIN/PUK-Transport

Ein Transport der PIN/PUK innerhalb des Systems ist zu verschiedenen Zwecken notwendig. Dazu gehört z. B. die Mitteilung der PIN durch den Kartenherausgeber bzw. Kartenpersonalisierer an den Karteninhaber[3] oder der Druck des PIN/PUK-Briefes. Die nachfolgenden Mindestanforderungen für den PIN/PUK-Transport müssen für jeden Transport eingehalten werden.

⌦ **GS-A_2253 PIN/PUK-Transport: Sicherer PIN-Transport beim Kartenherausgeber bzw. Kartenpersonalisierer**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die PIN/PUK in Transport und Speicherung vor nicht autorisierter Aufdeckung und Weitergabe geschützt wird.⌫

⌦ **GS-A_2254 PIN/PUK-Transport: Schutz außerhalb geschützter Hardware beim Kartenherausgeber bzw. Kartenpersonalisierer**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass PINs/PUKs außerhalb geschützter Hardware nicht unverschlüsselt auftreten. Ausnahme ist der einmalige Ausdruck des PIN/PUK-Briefes, der durch gesonderte organisatorische Maßnahmen gesichert ist.⌫

⌦ **GS-A_2255 PIN/PUK-Transport: Verteilung beschränken**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die Verteilung der PIN/PUK auf das absolut notwendige Maß eingeschränkt wird, um die Möglichkeiten zur Kompromittierung der PIN/PUK zu minimieren und potentielle Schäden zu beschränken.⌫

⌦ **GS-A_2256 PIN/PUK-Transport: einmalige PIN-Erstellung beim Kartenherausgeber bzw. Kartenpersonalisierer**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass eine PIN/PUK für den Transport nur erstellt wird, wenn dies erforderlich ist und direkt dem Karteninhaber übermittelt wird.⌫

⌦ **GS-A_2260 PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass während des elektronischen PIN/PUK-Transports außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls, die PIN verschlüsselt ist. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS sicherstellen, dass die dabei verwendeten kryptographischen Algorithmen die aktuellen Mindestanforderungen der gematik entsprechend [gemSpec_Krypt] erfüllen.⌫

[3] Dieses Unterkapitel betrifft nicht die Verteilung öffentlicher Transport-PINs bzw. Einmal-PINs, die nach der Eingabe durch den Karteninhaber zu ändern sind.

GS-A_2261 PIN/PUK-Transport: Transport außerhalb eines Sicherheitsmoduls - kein Klartext

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass eine PIN/PUK außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls nicht im Klartext erscheint. Ausnahme ist der Ausdruck des PIN/PUK-Briefes, der durch gesonderte organisatorische Maßnahmen zu sichern ist. ⌫

GS-A_2264 PIN/PUK-Transport: elektronische PIN-Verteilung

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass während der elektronischen PIN/PUK-Verteilung außerhalb einer sicheren Umgebung oder eines Sicherheitsmoduls die Integrität der PIN/PUK geschützt wird. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS sicherstellen, dass die dabei verwendeten kryptographischen Algorithmen die aktuellen Mindestanforderungen der gematik entsprechend [gemSpec_Krypt] erfüllen.⌫

GS-A_2266 PIN/PUK-Transport: Verschlüsselung gleicher PINs muss zu unterschiedlichen Werten führen

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass, falls zwei PINs einer Karte zufällig den gleichen Wert aufweisen, sie bei der Verschlüsselung zum Transport auf verschiedene verschlüsselte Werte abgebildet werden.⌫

GS-A_2270 PIN/PUK-Transport: Unterschiedliche verschlüsselte Werte auch bei gleichen PINs

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass falls zwei PINs unterschiedlicher Karten zufällig den gleichen Wert aufweisen, sie bei der Verschlüsselung zum Transport auf verschiedene verschlüsselte Werte abgebildet werden.⌫

GS-A_2271 PIN/PUK-Transport: kein Rückschluss auf vorher benutzte Schlüssel

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die Wahl der Schlüssel zum Schutz der PIN/PUK während der Verteilung so erfolgt, dass es nicht möglich ist, bei Kenntnis aller ab einem Zeitpunkt benutzten Schlüssel die vorher benutzten Schlüssel abzuleiten.⌫

GS-A_2274 PIN/PUK-Transport: Löschung der PIN nach Transport

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die PIN/PUK nach der Übertragung in den bei der Übertragung beteiligten und in seiner Verantwortung befindlichen Komponenten sicher gelöscht werden.⌫

Im BSI-Grundschutzbaustein M 2.167 „Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten“ oder in der Technischen Leitlinie des BSI "Richtlinien für das Löschen und Vernichten von schutzbedürftigen Informationen auf analogen und digitalen Datenträgern" sind Maßnahmenempfehlungen für sicheres Löschen beschrieben.

⌦ **GS-A_2276 PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip bei der Zuordnung einer PIN/PUK zu einer Karte**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass alle Aktivitäten und die unterstützenden Systemfunktionen der PIN/PUK-Herausgabe, die die Zuordnung einer PIN/PUK zu einer Karte oder zu einem Karteninhaber betreffen und die Personal des Herausgebers bzw. Personal des vom Kartenherausgeber beauftragten Kartenpersonalisierers benötigen, dem Vier-Augen-Prinzip gehorchen.⌫

⌦ **GS-A_2277 PIN/PUK-Transport: Aktivitäten im Vier-Augen-Prinzip beim Rücksetzen des Fehlbedienungszählers**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass alle Funktionen, die das Rücksetzen des Fehlbedienungszählers bzw. der (De)Aktivierung einer Karte oder Kartenanwendung betreffen und die Personal des Kartenherausgebers bzw. Kartenpersonalisierer benötigen, dem Vier-Augen-Prinzip gehorchen.⌫

2.4 PIN/PUK-Verwendung

An den Kartenherausgeber und den Kartenpersonalisierer werden bzgl. der Verwendung der PIN/PUK keine Anforderungen gestellt.

2.5 PIN -Änderung

Eine Änderung einer PIN kann aus mehreren Gründen notwendig sein:

- der Karteninhaber möchte die PIN wechseln,
- der Karteninhaber hat die PIN vergessen,
- die PIN ist (tatsächlich oder mutmaßlich) kompromittiert.

Für die Prozesse beim Kartenherausgeber bzw. Kartenpersonalisierer ergeben sich hieraus folgende Anforderungen:

⌦ **GS-A_2284 PIN/PUK-Änderung: Änderungen durch Kartenpersonalisierer im Vier-Augen-Prinzip**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass alle Prozesse einer PIN-Änderung, die Personal des Kartenherausgebers bzw. Kartenpersonalisierers benötigen, dem Vier-Augen-Prinzip gehorchen.⌫

⌦ **GS-A_2285 PIN/PUK-Änderung: Prozess bei Kompromittierung beim Kartenherausgeber bzw. Kartenpersonalisierer**

Falls der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer eine PIN/PUK von Kartendaten ableiten kann oder in anderer Weise zur Verfügung hat, MUSS er sicherstellen, dass, falls eine PIN/PUK beim Kartenherausgeber bzw. Kartenpersonalisierer kompromittiert wurde, die PIN/PUK beim Kartenherausgeber bzw. Kartenpersonalisierer so schnell wie möglich deaktiviert bzw. gesperrt wird. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS sicherstellen, dass es einen praktikablen Prozess gibt, um kompromittierte PIN/PUK beim Kartenherausgeber bzw. Kartenpersonalisierer zu sperren. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS den Karteninhaber über die Kompromittierung informieren.⌫

⌦ **GS-A_5085 PIN/PUK-Änderung: Prozess bei Kompromittierungsmeldung durch Karteninhaber**

Falls der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer eine PIN/PUK von Kartendaten ableiten kann oder in anderer Weise zur Verfügung hat, MUSS er sicherstellen, dass, falls eine PIN/PUK vom Karteninhaber als kompromittiert gemeldet wurde, die PIN/PUK beim Kartenherausgeber bzw. Kartenpersonalisierer so schnell wie möglich deaktiviert bzw. gesperrt wird. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS sicherstellen, dass es einen praktikablen Prozess gibt, um kompromittierte PIN/PUK beim Kartenherausgeber bzw. Kartenpersonalisierer zu sperren. Der Kartenherausgeber bzw. Kartenpersonalisierer MUSS den Karteninhaber über die Prozesse zur Sperrung von kompromittierten PIN/PUK informieren ⌫

2.6 PIN/PUK-Löschung

Die PIN/PUK darf nur für den vorgesehenen Zweck verwendet werden. Um missbräuchliche Verwendung und Kompromittierungsmöglichkeiten zu verringern, muss eine nicht mehr benötigte PIN/PUK daher in allen Komponenten unverzüglich sicher gelöscht werden. In der Regel sind die PINs/PUKs nach dem einmaligen Gebrauch unverzüglich zu löschen.

Für die ggf. notwendige Speicherung in zentralen Systemen in der Verantwortung des Kartenherausgebers bzw. des von ihm beauftragten Kartenpersonalisierers sind die folgenden Anforderungen mindestens einzuhalten.

⌦ **GS-A_2287 PIN/PUK-Löschung: Nachweis der Löschung nicht mehr gebrauchter PIN beim Kartenherausgeber bzw. Kartenpersonalisierer**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die unverzügliche sichere Löschung von nicht mehr benötigten elektronischen PINs/PUKs bzw. zugeordneten Schlüsseln in den Komponenten und Diensten, die in seiner Verantwortung sind, in seinem Sicherheitskonzept nachgewiesen wird. ⌫

⌦ **GS-A_2252 PIN/PUK-Löschung: Löschung von PIN/PUK nach Ablauf der Speicherdauer**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die PIN/PUK nach Ablauf der Speicherdauer in den Komponenten und Diensten, die in seiner Verantwortung sind, sicher gelöscht wird.⌫

⌦ **GS-A_2291 PIN/PUK-Löschung: Löschen von nicht mehr benötigten Klartext-PIN**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS Vorkehrungen treffen, um die nicht mehr benötigte Klartext-PIN/PUK so zerstören zu können, dass es nicht mehr möglich ist, die PIN/PUK ganz oder teilweise zu rekonstruieren. Insbesondere MÜSSEN die Kartenherausgeber bzw. Kartenpersonalisierer geeignete Sicherheitsmaßnahmen treffen in Bezug auf die interne Handhabung und Beseitigung von zurückgesendeten PIN/PUK-Briefen und Material, das mit dem ursprünglichen Druck der PIN/PUK-Briefe verbunden ist. Dabei MUSS der Kartenherausgeber bzw. Kartenpersonalisierer sicherstellen, dass die Behandlung zurückgesandter PIN/PUK-Briefe von der Behandlung der zurückgesandten Karten organisatorisch getrennt ist. ⌫

⌦ **GS-A_2292 PIN/PUK-Löschung: Außerbetriebnahme der PIN und Karte**

Der Kartenherausgeber MUSS die sichere Außerbetriebnahme der PIN und der damit verbundenen Karten regeln. Der Kartenherausgeber MUSS entsprechende praxistaugliche Verfahren festlegen.⌫

Hinweis: Auch abgelaufene Karten bergen Risiken z. B. auf der eGK vorhandene medizinische Daten wie etwa Notfalldaten sowie im HBA noch verwendbare C2C-Authentisierungsschlüssel, die einen Offline-Zugriff auf geschützte medizinische Daten ermöglichen.

3 Mindestanforderungen und Sicherheits-Policies für die Behandlung der Schlüssel zum Schutz der PIN/PUK

Das sichere Management der Schlüssel für die Behandlung der PIN/PUK ist entscheidend für die Einhaltung der Mindestanforderungen für PIN/PUK. Die Schlüsselverwendung und die nachfolgenden Bereiche des Schlüsselmanagements müssen die Mindestanforderungen der gematik erfüllen: Der Lebenszyklus der Schlüssel umfasst nach [ISO11770] die Schlüsselerzeugung (generation) mit Registrierung des Schlüssels bzw. des Zertifikats, die Schlüsselableitung, die Schlüsselaktivierung (activation) mit der Installation, jeweils optional die Zertifikatserzeugung, die Schlüsselverteilung, die Schlüsselspeicherung sowie die Schlüsseldeaktivierung (deactivation), die Reaktivierung (reactivation) und die Schlüsselzerstörung (destruction).

⌦ **GS-A_2295 Schutz der Schlüssel für PIN/PUK gemäß Hierarchiestufe 4**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass für die Schlüssel zum Schutz der PIN/PUK, die bei der Kartenproduktion verwendet werden, die organisatorischen und technischen Maßnahmen eingesetzt werden, die sicherstellen, dass

- nur autorisierte Personen das Schlüsselmaterial verwenden können,
- das Vier-Augen-Prinzip bei allen Operationen mit diesen Schlüsseln durchgesetzt wird,
- die Schlüssel nur innerhalb von Sicherheitsmodulen (Chip, HSM) im Klartext vorliegen,
- die Schlüssel mithilfe eines physikalischen Zufallsgenerators erzeugt werden,
- die Schlüssel eine bei der Erzeugung festzulegende maximale Lebensdauer besitzen, nach dieser sie zerstört werden müssen und
- die Schlüssel nur zweckbestimmt eingesetzt werden.⌫

Anhang A - Verzeichnisse

A1 - Abkürzungen

Kürzel	Erläuterung
C2C	Card to Card
CA	Certification Authority
eGK	elektronische Gesundheitskarte
HBA	(elektronischer) Heilberufsausweis
HSM	Hardware Sicherheits Modul
ISO	International Organization for Standardization
PIN	Persönliche Identifikationsnummer
PUK	Personal Unblocking Key
SMC	Security Module Card
TI	Telematikinfrastruktur

A2 - Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 - Referenzierte Dokumente

A3.1 – 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 entnehmen Sie bitte der aktuellsten, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

A3.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO11770]	ISO/IEC 11770: 1996 Information technology - Security techniques - Key management Part 3: Mechanisms using asymmetric techniques
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2119

© gematik - öffentlich