Einführung der Gesundheitskarte

Übergreifende Spezifikation PIN/PUK-Policy für Smartcards der Telematikinfrastruktur

|  |  |
| --- | --- |
| Version: | 1.2.0 |
| Revision: | \main\rel\_online\rel\_ors1\rel\_opb1\5 |
| Stand: | 28.10.2016 |
| Status: | freigegeben |
| Klassifikation: | öffentlich |
| Referenzierung: | [gemSpec\_PINPUK\_TI] |

Dokumentinformationen

Änderungen zur Vorversion

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 |
| 0.10.0 | 20.04.12 | Kap. 2.1,  Kap. 4 | Ergänzung Kapitel 2.1 und Einführung von Kapitel 4. | ITS/SI |
| 0.15.0 | 11.01.13 |  | Anpassung an die Inhalte und Struktur der vergaberelevanten Dokumente | ITS/SI |
| 0.19.0 | 22.04.13 |  | Einarbeitung Gesellschafterkommentare | P77 |
| 1.0.0 | 06.06.13 |  | freigegeben | gematik |
| 1.1.0 | 21.02.14 |  | Losübergreifende Synchronisation | P77 |
|  |  |  | Einarbeitung lt. Änderungsliste |  |
| 1.2.0 | 28.10.16 |  | freigegeben | gematik |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 5](#_Toc501717329)

[1.1 Zielsetzung 5](#_Toc501717330)

[1.2 Zielgruppe 5](#_Toc501717331)

[1.3 Geltungsbereich 5](#_Toc501717332)

[1.4 Abgrenzung 6](#_Toc501717333)

[1.5 Methodik 6](#_Toc501717334)

[2 Mindestanforderungen und Sicherheits-Policies für die Behandlung von PIN/PUK 7](#_Toc501717335)

[2.1 PIN/PUK-Erzeugung 8](#_Toc501717336)

[2.2 PIN/PUK-Speicherung 10](#_Toc501717337)

[2.3 PIN/PUK-Transport 12](#_Toc501717338)

[2.4 PIN/PUK-Verwendung 15](#_Toc501717339)

[2.5 PIN -Änderung 15](#_Toc501717340)

[2.6 PIN/PUK-Löschung 16](#_Toc501717341)

[3 Mindestanforderungen und Sicherheits-Policies für die Behandlung der Schlüssel zum Schutz der PIN/PUK 18](#_Toc501717342)

[4 Anhang A - Verzeichnisse 19](#_Toc501717343)

[4.1 A1 - Abkürzungen 19](#_Toc501717344)

[4.2 A2 - Glossar 19](#_Toc501717345)

[4.3 A3 - Referenzierte Dokumente 19](#_Toc501717346)

[4.3.1 A3.1 – Dokumente der gematik 19](#_Toc501717347)

[4.3.2 A3.2 – Weitere Dokumente 20](#_Toc501717348)

# Einordnung des Dokumentes

## Zielsetzung

Die übergreifende PIN/PUK-Policy für Smartcards der TI gilt für den Gesamtbereich Kar­ten­produktion, Kartenausgabe, Karten­ein­zug der eGK[[1]](#footnote-1) und der HBA[[2]](#footnote-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.

## 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.

## Geltungsbereich

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

## Abgrenzung

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

## 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.

# 

# 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

## 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.

**⌫**

## 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.

**⌫**

## 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]](#footnote-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.

**⌫**

**⌦ 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.

**⌫**

## PIN/PUK-Verwendung

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

## 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

**⌫**

## 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.

# 

# 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> |

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. [↑](#footnote-ref-1)
2. Die PINs für die qualifizierte elektronische Signatur eines HBA werden von der BNetzA geregelt und sind nicht Gegenstand dieses Dokumentes. [↑](#footnote-ref-2)
3. Dieses Unterkapitel betrifft nicht die Verteilung öffentlicher Transport-PINs bzw. Einmal-PINs, die nach der Eingabe durch den Karteninhaber zu ändern sind. [↑](#footnote-ref-3)