gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Beschreibung der zulässigen PIN- und PUK-Verfahren für die eGK

Version:	1.2.0
Stand:	25.03.2008
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Es wurde festgelegt, dass sowohl für PIN.CH als auch für PIN.home nur bei der Erstausgabe neben dem Versand eines Briefes mit der Echt-PIN die Nutzung einer Leer-PIN (in den beschriebenen technischen Varianten) zulässig ist. Für Folgekarten darf keine Leer-PIN verwendet werden. Das Dokument wurde entsprechend angepasst. Zusätzlich wird an mehreren Stellen auf die zu berücksichtigenden Dokumente und die Verantwortung der Kostenträger für den Gesamtprozess der PIN-Verfahren hingewiesen.

Die Änderungen gegenüber der Vorversion sind gelb markiert. Bei Ergänzungen von Kapiteln oder Abschnitten wurde der besseren Lesbarkeit wegen lediglich die Überschrift markiert.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemCMS_PINPUK]	gematik (25.03.2008): Einführung der Gesundheitskarte - Beschreibung der zulässigen PIN- und PUK-Verfahren für die eGK Version 1.2.0

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.1	26.6.06		Neues Dokument	gematik, AG3
0.1.1	14.09.06		Umarbeitung nach Kommentaren	gematik, AG3
0.1.3	27.09.06		Einarbeitung von Änderungsvorschlägen	gematik, AG3
0.1.4	02.10.06		Einarbeitung Unterscheidung PIN.home und PIN.CH	gematik, AG3
0.1.7	16.10.06		Einfügen modifiziertes Verfahren zur PUK-Übertragung	gematik, AG3
0.1.8	26.10.06		Einarbeitung Kommentare zu modifiziertem Verfahren zur PUK-Übertragung	gematik, AG3
0.9.0	23.10.06		Freigegeben zur Vorkommentierung	gematik
0.9.1	19.12.06		Einarbeitung der Ergebnisse des Vorkommentierungsverfahrens	gematik, AG3
1.0.0	20.12.06		Freigegeben	gematik
1.0.1	19.11.07	4.2.3.1 4.2.3.2	Anforderung der Festlegung eines Verfahrens zur Ermittlung eines Wertes für die Transport-PIN, Das Null-PIN-Verfahren wird nicht mehr	SPE/DK

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
		4.4.4.2	gesondert beschrieben, da es ein Spezialfall der Transport-PIN mit festem, bekanntem Wert ist	
1.0.3	20.12.07		Anpassung an eGK-Spezifikation Teil 2 und zugelassene Transport-PIN-Verfahren Editorische Präzisierungen	SPE/DK
1.1.0	20.12.07		freigegeben	gematik
1.1.1	02.02..08		Anpassung an eine Erweiterung der zugelassenen PIN-Verfahren für PIN.CH	SPE/DK
1.1.4	17.02.08		Einarbeitung der Kommentare	SPE/DK
1.1.7	17.03.08		Einarbeitung Entscheidung zu Folgekarten	SPE/DK
1.2.0	25.03.08		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Die Freischaltung der privaten Schlüssel (ENC, AUT und ggf. QES), die auf der eGK gespeichert sind, erfolgt durch die Eingabe von PINs (Personal Identification Number). Zusätzlich werden weitere Funktionen durch Eingabe einer PIN freigeschaltet, z.B. das Lesen der Protokoll-Records auf der eGK durch den Karteninhaber. Die PIN-Werte dürfen nur dem Karteninhaber bekannt gemacht werden. Es gibt verschiedene Verfahren, diese PINs (und, falls genutzt, auch die zugehörigen PUKs (Personal Unblocking Key)) dem Karteninhaber bei Ausgabe der Karte mitzuteilen bzw. ihm die Bestimmung einer individuellen PIN zu ermöglichen.

In diesem Dokument werden die verschiedenen Verfahren der PIN- und PUK-Übermittlung beschrieben, die von der gematik gestattet werden.

Die Verantwortlichkeit für den Gesamtprozess liegt entsprechend [gemSiKo] bei den Kartenherausgebern.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Die Kartenherausgeber müssen bei der Auslieferung der Gesundheitskarte auch für die Übermittlung der zur Aktivierung verschiedener Funktionen benötigten PINs und PUKs sorgen. Aus technischer Sicht gibt es dafür verschiedene Verfahren mit spezifischen Vor- und Nachteilen. Dabei gilt es, Sicherheitsanforderungen, Kosten für die Verteilung und mögliche Auswirkungen auf die Nutzerakzeptanz gegeneinander abzuwägen. Dieses Dokument gibt den Kostenträgern eine Entscheidungshilfe bei der Auswahl des Verfahrens zur Festlegung und zum Versand von PINs und PUKs und definiert gleichzeitig den zulässigen Handlungsrahmen auf Basis des festgelegten übergreifenden-Sicherheitskonzeptes [gemSiko] und [gemSiko#AnhF].

2.2 Zielgruppe

Dieses Dokument wendet sich an die Kostenträger, die Aufträge zur Erstellung und zum Versand der eGK und der dazugehörenden PINs und PUKs erteilen.

2.3 Geltungsbereich

Dieses Dokument gilt für den Gesamtbereich der eGK-Ausgabe und -Nutzung bei der Erstausgabe und der Ausgabe von Folgekarten.

2.4 Arbeitsgrundlagen

Das Dokument basiert auf den Vorgaben, die sich aus [gemSpec_eGK_P1] und [gemSpec_eGK_P2] bezüglich der Eigenschaften der PINs ergeben, und ergänzt diese Vorgaben um Punkte, die die Erzeugung und die Verteilung der PINs und PUKs an den Karteninhaber betreffen. Weiter sind Vorgaben aus [gemSiKo] einschließlich der darauf basierenden PIN/PUK-Policy [gemSiKo#AnhE] und [gemGesArch] zu erfüllen, und es ist die Schutzbedarfsfeststellung aus [gemSiKo#AnhC] zu berücksichtigen.

2.5 Abgrenzung des Dokumentes

Die Sicherheitsvorgaben (Qualität der erzeugenden Einheiten, Sicherung bei Erzeugung, Transport und Speicherung) sind nicht Gegenstand dieses Dokumentes, sondern werden in den Dokumenten [gemPers_krypt] und [gemSiKo] festgelegt. Entsprechend der Sicherheitsverantwortlichkeit der Kostenträger für den Gesamtprozess sind die verbleibenden Restrisiken von den Kostenträgern in ihrem Sicherheitskonzept zu bewerten und zu übernehmen.

Vorgaben für die Erzeugung und Verteilung einer PIN für die QES sind nicht Gegenstand dieses Dokumentes.

2.5.1 Verwendung von Schlüsselworten

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

- **MUSS** bedeutet, dass es sich um eine absolutgültige und normative Festlegung bzw. Anforderung handelt.
- **DARF NICHT** bezeichnet den absolutgültigen und normativen Ausschluss einer Eigenschaft.
- **SOLL** beschreibt eine Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich.
- **SOLL NICHT** kennzeichnet die Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich.
- **KANN** bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

2.5.2 Namenskonvention

In diesem Dokument werden die technischen Namen der beschriebenen PINs (PIN.home und PIN.CH) verwendet. Gemäß AR 0586 werden diese technischen Namen in der Kommunikation mit dem Nutzer wie folgt dargestellt:

PIN.home: Privat-PIN

PIN.CH: Praxis-PIN

3 Anforderungen und Annahmen

Es werden die verschiedenen Möglichkeiten für die Erzeugung und Verteilung von PIN und PUK beschrieben. Dabei MUSS der Kartenherausgeber die übergreifenden Sicherheitsanforderungen [gemSiko], [gemSiKo#AnhE] und die in dem Dokument [gemPers_krypt] beschriebenen Vorgaben als Mindestanforderungen einhalten.. Bei der Datenverarbeitung im Auftrag des Kostenträgers (z.B. Kartenproduzent) KANN dies auch durch die jeweiligen Sicherheitskonzepte der Auftragsdatenverarbeiter nachgewiesen werden.

Die Verantwortlichkeit für die Sicherheit der Ausgabeprozesse liegt bei den Krankenkassen und privaten Krankenversicherungen für die eGK (siehe [gemSiko#9]) und die getroffenen Maßnahmen des Sicherheitskonzepts der Kasse sind bezüglich der Wirksamkeit zu bewerten und die verbleibenden Restrisiken zu übernehmen.

Zu den Sicherheitsbedingungen, die von den verschiedenen Verfahren zur Erzeugung, Speicherung, Verteilung und Verwendung der PINs, PUKs erfüllt werden müssen, gehören allgemein:

Tabelle 1: Anforderungen an die PIN-/PUK-Verfahren

Kennung	Anforderung
A_01936	Bei Ausgabe einer eGK UND wenn der Karteninhaber keine freiwillige Anwendungen nutzt, MUSS die Auslieferung an den Versicherten mit einem der folgenden Verfahren erfolgen: * Echt PIN Verfahren mit PIN Brief: (Versand der eGK mit kartenindividuellen Echt-PINs für Privat-PIN und für Praxis-PIN mit gesonderter Zusendung der zugehörigen PIN Briefe.) * Transport PIN Verfahren mit Leer PIN: (Versand der eGK ohne nutzbare Privat-PIN und Praxis-PIN. Vor der ersten Nutzung müssen die PINs vom Karteninhaber initialisiert werden.)
A_01937	Bei Ausgabe einer eGK UND wenn der Karteninhaber freiwillige Anwendungen nutzt, MUSS die Auslieferung an den Versicherten mit dem folgenden Verfahren erfolgen: * Echt PIN Verfahren mit PIN Brief: (Versand der eGK mit kartenindividuellen Echt-PINs für PIN.CH und für PIN.Home mit gesonderter Zusendung der zugehörigen PIN Briefe.)
A_02241	Der Zugriff auf schützenswerte und PIN-geschützte personenbezogene und medizinische Daten des Karteninhabers durch Unberechtigte MUSS verhindert werden.
A_02242	Der Schutzbedarf dieser personenbezogenen Daten ist „sehr hoch“. Daher MÜSSEN die PINs, PUKs während des gesamten Lebenszyklus (Erzeugung, Speicherung, Verteilung, Verwendung, Löschung) entsprechend geschützt werden.
A_02243	Es MUSS durch technische und organisatorische Maßnahmen sichergestellt werden, dass die für den Zugriff auf schützenswerte und PIN-geschützte Daten verwendete PIN nur dem Karteninhaber bekannt

	ist. Die Maßnahmenstärke dieser technischen und organisatorischen Sicherheitsmaßnahmen ist für PINs und PUKs „sehr hoch“.
A_02244	Falls kartenindividuelle PINs/PUKs durch Ableitungsverfahren aus Masterkeys gewonnen werden, MÜSSEN diese Schlüssel mit technischen und organisatorischen Sicherheitsmaßnahmen der Mechanismenstärke „sehr hoch“ geschützt werden.
A_02245	Falls kartenindividuelle PINs/PUKs durch Ableitungsverfahren aus Masterkeys gewonnen werden, MÜSSEN bei Kompromittierung dieser Schlüssel alle betroffenen Karten unverzüglich getauscht werden.

4 PIN- und PUK-Verfahren

4.1 Spezifikation von PIN und PUK

Das Format von PIN und Resetting Code ist in [gemSpec_eGK_P1#9.1.7] beschrieben.

In [gemSpec_eGK_P2#6.2.7] und [gemSpec_eGK_P2#6.2.8] werden Details und Zugriffsregeln für PIN.CH und PIN.home beschrieben:

Die PIN-Charakteristika zeigt Tabelle 2.

Tabelle 2: PIN-Referenzen und Resetting Code

PIN Name	PIN Länge	PIN Referenz	Anfangswert des Retry Counters	Resetting Code	Nutzungs-begrenzung für Resetting Code
PIN.CH	6 - 8 Ziffern	‘01’	3	8 Ziffern	10
PIN.home	6 - 8 Ziffern	‘02’	3	8 Ziffern	10

Anmerkung: Nur die Mindestlänge wird von der eGK kontrolliert.

Wenn die eGK an den Karteninhaber ausgehändigt wird, kann als Transport-PIN-Verfahren ein Leer-PIN-Verfahren angewandt werden.

Es ist damit vorgegeben, dass die eGK zwei PINs enthalten MUSS (alle folgenden Betrachtungen lassen das Vorhandensein bzw. die Aktivierung einer qualifizierten elektronischen Signatur mit eigener PIN.QES außer Acht, da hierfür die im jeweiligen Sicherheitskonzept des ZDA festgelegten Regeln für Handling und Eigenschaften von PIN und PUK gelten). Die durch eine PIN geschützten Funktionen bleiben gesperrt, wenn diese PIN drei Mal hintereinander falsch eingegeben wurde. Eine weitere Eingabe der PIN ist dann nicht mehr möglich. Durch die zugehörende PUK (Resetting Code in Tabelle 2) kann die Sperrung bis zu 10-mal wieder aufgehoben und die PIN dabei auf einen neuen Wert gesetzt werden.

Die PIN.CH wird zum Anlegen und Nutzen freiwilliger Anwendungen (und zur Freischaltung der privaten Schlüssel PrK.CH.ENC und PrK.CH.AUT) in der Gesundheitstelematik genutzt. Bei der Erstausgabe einer eGK werden mit dieser PIN noch keine medizinischen Daten geschützt, da noch keine freiwilligen Anwendungen angelegt sind.

Die PIN.home dient der Wahrnehmung der Patientenrechte an einem PC und zur Freischaltung der privaten PKI-Schlüssel PrK.CH.ENC und PrK.CH.AUT außerhalb der Gesundheitstelematik. Sie wird benötigt, falls der Karteninhaber eine der genannten Anwendungen nutzen will.

Beide PINs darf nur der berechtigte Karteninhaber nutzen.

[gemSpec_eGK_P1] und [gemSpec_eGK_P2] enthalten keine Vorgaben für die Erzeugung und die Übermittlung der PINs und PUKs an den Nutzer. Auch die Fragen, wer PINs und PUKs erzeugt, wer sie in die Karte einbringt und wer sie zum Karteninhaber transportiert, sind nicht Gegenstand der Spezifikation und deshalb zwischen Kostenträger und Kartenhersteller zu klären. Die mindestens einzuhaltenden Sicherheitsvorgaben (Qualität der erzeugenden Einheiten, Sicherung bei Erzeugung, Transport und Speicherung) sind nicht Gegenstand dieses Dokumentes, sondern werden in den Dokumenten [gemPers_krypt] und [gemSiKo] festgelegt. Entsprechend der Sicherheitsverantwortlichkeit der Kasse für den Gesamtprozess sind die verbleibenden Restrisiken von der Kasse in ihrem Sicherheitskonzept zu bewerten und zu übernehmen.

Die von der gematik gestatteten Verfahren werden in diesem Dokument beschrieben.

4.2 PIN-Verfahren

4.2.1 PIN-Erzeugung bei der Herstellung, PIN zufällig und nicht reproduzierbar

Bei der Produktion steht eine mindestens 6-stellige, maximal 8-stellige Zufallszahl zur Verfügung und wird als PIN im entsprechenden File der eGK abgelegt. Diese PIN kann sowohl vom Kostenträger als auch vom Kartenhersteller erzeugt werden und ist dann gesichert in die Karte und den PIN-Brief zu bringen.

Zur Übermittlung der PIN an den Karteninhaber wird die PIN in einem gesonderten PIN-Brief an den Karteninhaber geschickt. Der PIN-Brief kann unmittelbar nach Versand der Karte oder auch später auf Anforderung durch den Versicherten verschickt werden.

Normalerweise wird die PIN nach dem Versenden des PIN-Briefes sicher gelöscht. Da die PIN in diesem Fall jedes Mal wieder als Zufallszahl generiert wird, erhält jede neue Karte des Karteninhabers eine neue PIN. Diese muss wieder per PIN-Brief übermittelt werden.

Falls die PIN vom Kostenträger gespeichert werden soll (um dem Nutzer beim Ausstellen einer Folgekarte dieselbe PIN zuweisen zu können), muss organisatorisch und technisch gewährleistet werden, dass sie sicher gespeichert und nur für den vorgesehenen Zweck verwendet wird. Die PIN muss sicher und nicht auslesbar an den Produzenten der Karte und an den Produzenten des PIN-Briefes übermittelt und mit der richtigen Karte bzw. den richtigen Briefdaten verbunden werden

4.2.2 PIN-Erzeugung bei der Karten-Herstellung, PIN abgeleitet

Für die Produktion wird die mindestens 6-stellige, maximal 8-stellige PIN aus Daten abgeleitet, die dem Kostenträger bekannt sind. Es muss organisatorisch/technisch sichergestellt werden, dass eine PIN nur für den vorgesehenen Zweck berechnet wird. Dieses Verfahren kann sowohl beim Kostenträger als auch beim Kartenhersteller zur Anwendung kommen. Die Regeln für die Ableitung der PIN sind im Sicherheitskonzept der erzeugenden Stelle festzulegen.

Da in diesem Fall die PIN abgeleitet wird, kann eine neue Karte des Karteninhabers dieselbe PIN enthalten.

Ansonsten gelten die Ausführungen von Abschnitt 4.2.1.

4.2.3 Transport-PIN

4.2.3.1 Leer-PIN

Es werden nur Transport-PIN-Verfahren gestattet, bei denen der Versicherte bei der Umwandlung des Transport-Status in den Wirk-Status keinen Transport-PIN-Wert eingeben muss. Hierzu gehören zwei Leer-PIN-Verfahren, die sich durch die Eingabeparameter im Kommando unterscheiden, und das Transport-PIN_0000 genannte Verfahren, bei dem bei der Umwandlung im entsprechenden Kommando die Zeichenfolge '0000' an die eGK gesendet wird (siehe [gemSpec_eGK_P1], Tabelle 8). Alle drei Verfahren werden in diesem Dokument unter dem Begriff „Leer-PIN" zusammengefasst.

Der Konnektor kann das gewählte Verfahren nach Abfrage an dem Wert des Attributstyps *transportStatus* erkennen und eine dem genutzten Verfahren entsprechende Kommandosequenz auslösen (siehe [gemSpec_eGK_P1], Kapitel 9.2.5).

Der Versicherte muss bei diesen Verfahren seine PIN durch zweimalige Eingabe einer von ihm gewählten Echt-PIN vorgegebener Länge (wie spezifiziert: 6 bis 8 Stellen) aktivieren.

Es muss kein separater PIN-Brief verschickt werden.

Hinweis: Transport-PIN-Verfahren können patentrechtlich geschützt sein; dies ist entsprechend zu berücksichtigen.

4.2.4 Übersicht aller gestatteten Verfahren

Tabelle 3: Übersicht PIN-Verfahren

	Echt-PIN		Transport-PIN		
	Zufallswert	Abgeleiteter Wert	Transport-PIN_0000	Leer-PIN 1	Leer-PIN 2
separater PIN-Brief muss verschickt werden	X	X	-	-	-
Kartenherausgeber kann PIN erzeugen	X	X	-	-	-
Kartenproduzent kann PIN erzeugen	X	X	-	-	-

4.3 Anforderungen für die Behandlung PIN/PUK

4.3.1 Mindestanforderungen PIN/PUK-Erzeugung

Die PINs/PUKs MÜSSENS während des gesamten Lebenszyklus entsprechend der Schutzbedarfsfeststellung aus [gemSiKo#AnhC] und der darauf basierende PIN/PUK-Policy [gemSiKo#AnhE] geschützt werden. „Die Verantwortlichkeit für die Sicherheit der Ausgabeprozesse der PIN/PUK bis zur Übergabe an den Versicherten liegt bei den Krankenkassen und privaten Krankenversicherungen für die eGK (siehe [gemSiko#9]) und die getroffenen Maßnahmen des Sicherheitskonzepts der Kasse sind bezüglich der Wirksamkeit zu bewerten und die verbleibenden Restrisiken zu übernehmen."

Bei dieser Kosten/Nutzen/Risiken-Betrachtungen der Kasse sind die notwendigen zusätzlichen Komponenten des Kartenmanagements zu berücksichtigen und z.B. mögliche Einsparungen bei dem Versand der PIN-Briefe gegen die Kosten der dafür notwendigen Komponenten beim Kartenherausgeber und die Kosten zusätzlich notwendiger Identifikationsverfahren bei der Nutzung der verschiedenen PIN-Verfahren abzuwägen und gegen die verbleibenden Restrisiken einer möglichen unberechtigten Nutzung der Karte bzw. eines unberechtigten Zugriffs der Folgekarte zugeordneten personenbezogenen oder medizinischen Daten zu bewerten..

4.3.2 PIN/PUK-Speicherung

Die Speicherung von PINs/PUKs beim Kartenherausgeber findet i.d.R. für den Produktionsprozess bis zur Speicherung auf der Karte statt. Zusätzlich kann eine Speicherung über den Lebenszyklus einer Karte hinaus erfolgen, falls der Herausgeber die PINs/PUKs für die Ausgabe von Folgekarten bzw. für zentrale Rücksetzung des Fehlbedienungszählers nach der Kartenausgabe verwenden will – z.B. zum Einsparen von Portokosten durch nur einmalige Versendung eines PIN-Briefes. Die gespeicherte PIN/PUK darf nicht abgehört oder unbemerkt manipuliert werden können. PINs/PUKs dürfen nur innerhalb von Sicherheitsmodulen (Chipkarte oder HSM) und Sicherheitsobjekten (inkl. PIN-Brief) im Klartext vorliegen. Die Stärke der technischen und organisatorischen Maßnahmen zum Schutz der PIN MUSS sehr hoch sein.

4.3.3 PIN/PUK Transport

Ein Transport der PIN/PUK ist zu verschiedenen Zwecken notwendig. Dazu gehört z. B. die Mitteilung der PIN an den Karteninhaber durch den Herausgeber, die Verteilung der PIN/PUK vom Kartenherausgeber an Dienstleister für die Kartenpersonalisierung oder der Druck des PIN/PUK-Briefes. Die nachfolgenden Mindestanforderungen für den PIN/PUK Transport MÜSSEN für jeden Transport eingehalten werden:

Während der PIN-Verteilung DARF die PIN NICHT abgehört oder unbemerkt manipuliert werden können. Außerdem MUSS sichergestellt werden, dass die PIN nicht von Unbefugten dem zugehörigen Versicherten zugeordnet werden kann. Eine unberechtigte Zwischenspeicherung und unberechtigte nachträgliche Verwendung der PIN (u. A. Ausdruck eines zweiten PIN-Briefes für einen anderen Adressaten) MUSS verhindert werden.

4.3.4 PIN/PUK-Verwendung

Die Verwendung der PIN/PUK erfolgt gemäß der Beschreibung in [gemSpec_eGK_P1] und [gemSpec_eGK_P2]. Bei der Eingabe der PIN durch den Versicherten DARF die PIN NICHT außerhalb der Karte (z.B. in einem Terminal) gespeichert werden.

4.3.5 PIN-Änderung

Gemäß der Beschreibung in [gemSpec_eGK_P1] und [gemSpec_eGK_P2] kann der Versicherte seine PINs ändern.

4.4 Einordnung der verschiedenen Verfahren für die PIN

Für die verschiedenen Verfahren gelten die folgenden Anmerkungen bezüglich der Sicherheit des jeweiligen Verfahrens.

4.4.1 Allgemeine Anmerkungen

Bei der Ausgabe einer eGK ist noch nicht klar, wann eine PIN-geschützte Anwendung erstmals genutzt wird. Damit kann zwischen Zusendung der Karte (und ggf. Zusendung des PIN-Briefes) und der ersten Nutzung einer der PIN-geschützten Funktionen der eGK durch den Versicherten ein erheblicher Zeitraum liegen. Es besteht deshalb die Gefahr, dass der Versicherte die erforderliche Information zum Zeitpunkt der erstmaligen Nutzung freiwilliger Anwendungen in der Praxis des Arztes nicht verfügbar hat.

Dieses Problem kann durch die Nutzung der Leer-PIN als Transportschutz gelöst werden: vor der ersten Nutzung PIN-geschützter Funktionen der eGK muss der Karteninhaber nur die von ihm gewählte PIN eingeben, um die PIN zu aktivieren. Funktioniert die Umwandlung in dieser Weise, ist zusätzlich sichergestellt, dass die PIN-geschützten Funktionen vorher noch nicht genutzt wurden. Funktioniert die Umwandlung nicht, dann ist sie schon vorher erfolgt. Dies kann auf eine missbräuchliche Umwandlung und Nutzung der Karte hindeuten.

4.4.2 PIN-Erzeugung bei der Herstellung, PIN zufällig und nicht reproduzierbar

4.4.2.1 Keine Speicherung der PIN beim Herausgeber

In diesem Fall ist durch Erzeugung einer Zufallszahl, die dem Nutzer durch einen separaten PIN-Brief übermittelt wird und die nach der Produktion außer in der Karte und im PIN-Brief nirgends gespeichert ist, eine hohe Sicherheit gegen Missbrauch gegeben.

Die PIN-geschützten Bereiche der Karte sind nach Erhalt des PIN-Briefes sofort nutzbar.

4.4.2.2 Speicherung der PIN beim Herausgeber

Die Speicherung der PIN kann notwendig sein, falls der zugehörige PIN-Brief zu einem späteren Zeitpunkt erst auf Anfrage an den Karteninhaber gesendet werden soll.

In diesem Fall ist durch Erzeugung einer Zufallszahl, die dem Nutzer durch einen separaten PIN-Brief übermittelt wird, eine hohe Sicherheit gegen Missbrauch gegeben. Es muss organisatorisch/technisch sichergestellt werden, dass die PIN sicher gespeichert und nur für den vorgesehenen Zweck verwendet wird

Die PIN-geschützten Bereiche der Karte sind nach Erhalt des PIN-Briefes sofort nutzbar.

4.4.3 PIN-Erzeugung bei der Herstellung, PIN abgeleitet

Bei der Erzeugung einer abgeleiteten PIN ist die Rekonstruktion der PIN immer wieder möglich. Damit muss jede neuerliche Ableitung (z.B. bei Erstellung einer Folgekarte) unter genau festgelegten und kontrollierten Bedingungen erfolgen.

Die PIN-geschützten Bereiche der Karte sind nach Erhalt des PIN-Briefes sofort nutzbar.

4.4.4 Transport-PIN

4.4.4.1 Leer-PIN

Es sind nur Transport-PIN-Verfahren gestattet, die bei der Umwandlung der eGK vom Transport-Status in den Wirk-Status keine Eingabe einer speziellen Transport-PIN erfordern (siehe Tabelle 3). Jeder, der als erster in den Besitz der Karte kommt, kann sie durch Eingabe einer selbstgewählten Echt-PIN aktivieren und damit benutzen. Es muss weder ein PIN-Brief verschickt werden noch muss sich der Nutzer eine PIN/Transport-PIN merken, um PIN-geschützte Funktionen aktivieren zu können.

Bei der Umwandlung verlangt das Terminal eine 2-malige Eingabe der selbst gewählten Echt-PIN.

Ein Missbrauch ist möglich, wenn die Karte in den Besitz eines Unbefugten gelangt, besonders, wenn der rechtmäßige Empfänger der Karte selten zum Arzt geht und den Verlust nicht umgehend bemerkt und anzeigt.

Bei Signaturkarten wird das Problem dadurch gelöst, dass der rechtmäßige Empfänger durch eine Rückmeldung an den ZDA den Empfang der Karte bestätigen muss, bevor diese in den Verzeichnisdienst aufgenommen und damit nutzbar wird. Aufgrund der hohen Sicherheitsanforderungen für die Gesundheitskarte und den Schutz gegen Missbrauch SOLL der Empfang der Karte bestätigt werden. Dies kann z.B. beim ersten Einsatz der Karte in der Praxis eines Arztes, beim Abholen der Karte beim Kostenträger oder durch andere geeignete Verfahren erreicht werden.

4.5 Regeln für die Nutzung der gestatteten PIN-Verfahren

Zu den Sicherheitsbedingungen, die von den verschiedenen Verfahren zur Verteilung der PINs erfüllt werden müssen, gehören allgemein:

(1) Der Zugriff auf schützenswerte und PIN-geschützte Daten des Karteninhabers durch Unberechtigte muss verhindert werden.

(2) Es muss sichergestellt werden, dass die für den Zugriff auf schützenswerte und PIN-geschützte Daten verwendeten PINs nur dem Karteninhaber bekannt gemacht werden.

Aus diesen Anforderungen lässt sich ableiten, dass Transport-PIN-Verfahren mit Leer-PIN nur genutzt werden dürfen, wenn die Karte im Transport-Zustand noch keine schützenswerten und durch eine der beiden PINs geschützten Daten enthält bzw. keine Daten in der IT-Infrastruktur gespeichert sind, für die der Zugriff durch PIN-geschützte Mechanismen gesichert ist.

4.5.1 Erstausgabe der eGK

Die Nutzung einer kartenindividuellen PIN, die dem Karteninhaber mit einem gesonderten PIN-Brief übermittelt wird, erfüllt die gestellten Anforderungen. Für das Verfahren der Transport-PIN als Leer-PIN gelten die folgenden Randbedingungen.

4.5.1.1 PIN.home

Die eGK enthält laut Spezifikation bei Ausgabe im Container EF.GVD geschützte Versichertendaten. Der Zugriff auf diese Daten ist nur nach Card-2-Card-Authentifizierung mit bestimmten Profilen und für den Versicherten auch nach Eingabe der PIN.home möglich (siehe [gemSpec_eGK_P2]).

In der Einführungsphase der eGK sind diese Daten zusätzlich im frei auslesbaren Container EF.VD gespeichert, um das Auslesen auch dort zu ermöglichen, wo noch keine Card-2Card-Authentisierung möglich ist.

Durch Eingabe der PIN.home kann der Versicherte die Nutzung der privaten Schlüssel für ENC und AUT freischalten. Hiermit sind bei Erstausgabe der eGK noch keine Anwendungen verbunden.

Für die PIN.home DARF bei Erstausgabe der eGK neben dem Versand einer Echt-PIN in einem separaten PIN-Brief auch ein Leer-PIN-Verfahren genutzt werden. Bei der ersten Nutzung der PIN.home MUSS bei Nutzung der LEER-PIN die Eingabe der Echt-PIN durch den berechtigten Besitzer erfolgen. Die Prüfung, ob der Besitzer der Karte der berechtigte Besitzer ist, muss durch geeignete organisatorische Verfahren sichergestellt werden.

4.5.1.2 PIN.CH

Die eGK enthält bei der Erstausgabe keine freiwilligen Anwendungen, deren Nutzung durch PIN.CH geschützt werden müsste.

Für die PIN.CH DARF bei Erstausgabe der eGK neben dem Versand einer Echt-PIN in einem separaten PIN-Brief auch ein Leer-PIN-Verfahren genutzt werden. Bei der ersten Nutzung der Karte MUSS bei Nutzung der LEER-PIN die Eingabe der Echt-PIN durch den berechtigten Besitzer erfolgen.

Die Prüfung, ob der Besitzer der Karte der berechtigte Besitzer ist, MUSS durch geeignete organisatorische Verfahren sichergestellt werden.

4.5.2 Folgekarten

Bei der Versendung von Folgekarten darf sowohl für PIN.home als auch für PIN.CH ein Transport-PIN-Verfahren NICHT mehr verwendet werden. Der versetzte Postversand von Karte und PIN-Brief für Folgekarten ist allerdings mit Risiken behaftet. Diese müssen von den Kartenherausgebern entsprechend bewertet und getragen werden. Es empfiehlt sich ein vorbeugender Ausschluss einer unberechtigten Nutzung durch eine Identifizierung und Aktivierung der eGK im Feld (z.B. bei Leistungserbringer bzw. Kasse)..

4.6 Beschreibung und Bewertung der verschiedenen Verfahren für die PUK

4.6.1 PUK-Erzeugung bei der Herstellung, PUK zufällig und nicht reproduzierbar

4.6.1.1 Keine Speicherung der PUK

In diesem Fall ist durch Erzeugung einer Zufallszahl, die dem Nutzer mit dem separaten PIN-Brief übermittelt wird und die nach der Produktion außer in der Karte und im PIN-Brief nirgends gespeichert ist, eine hohe Sicherheit gegen Missbrauch gegeben.

Der PIN/PUK-Brief muss vom Karteninhaber sorgfältig verwahrt werden, damit die PIN nicht ausgespäht werden kann, die PUK bei Bedarf aber zur Verfügung steht.

4.6.1.2 Speicherung der PUK beim Kostenträger

Alternativ kann die erzeugte Zufallszahl (PUK) auch bei der Herstellung an den Kostenträger übermittelt und von diesem unter Einhaltung definierter Sicherheitsbedingungen gespeichert werden. In diesem Fall kann die PUK nach Anforderung durch den Versicherten in einem definierten und den Sicherheitsanforderungen entsprechenden Verfahren an den Karteninhaber übermittelt werden. Um die Sicherheit der PUK zu gewährleisten, MÜSSEN die Vorgaben des Sicherheitskonzepts für das Schlüsselmanagement, speziell [gemSiKo#AnhE] und [gemSiKo#AnhF], und [gemPersKrypt] bei der Behandlung geheimer Schlüssel durch den Kostenträger eingehalten werden.

4.6.2 PUK-Erzeugung bei der Herstellung, PUK abgeleitet

Bei der Erzeugung einer abgeleiteten PUK ist die Rekonstruktion der PUK durch den Kostenträger immer wieder möglich. Jede neuerliche Ableitung (z.B. bei Abforderung durch den Karteninhaber) MUSS unter genau festgelegten und kontrollierten Bedingungen erfolgen.

Bei einer abgeleiteten PUK ist nicht zwingend erforderlich, dass diese bei Kartenausgabe erzeugt und an den Karteninhaber übermittelt wird. Die Erzeugung und Übermittlung nach Anforderung durch den Versicherten MUSS mit einem definierten und den Sicherheitsanforderungen entsprechenden Verfahren erfolgen.

In diesem Fall hängt die Sicherheit der PUK von der Einhaltung der Sicherheitsvorgaben für die Behandlung geheimer Schlüssel durch den Kostenträger ab (siehe [gemPersKrypt].

4.7 Ablaufbeschreibungen

Die Ausgabeprozesse der eGK müssen an die spezifische Verwendung der Gesundheitskarte angepasst werden. Ausgabeprozesse von Banken- oder Signaturkarten sind dabei nur bedingt übertragbar, da die Nutzungscharakteristika dieser Karten völlig unterschiedlich sind:

(1) Eine Signaturkarte wird in der Heimumgebung des Signaturkarteninhabers verwendet. Der Antragsteller hat ein hohes persönliches Interesse an der sofortigen Freischaltung und Verwendung der Karte.

(2) Bankenkarten werden an Terminals, Geldautomaten oder SB-Geräten eingesetzt bzw. spezifische Karten für Homebanking (HBCI) in einer Heimumgebung des Kunden. Der Kunde hat ein hohes Interesse, seine Geldgeschäfte mit dieser Karte abzuwickeln.

4.7.1 PIN.CH

Die eGK wird i.d.R. erst bei der Inanspruchnahme einer medizinischen Leistung des Versicherten beim Leistungserbringer verwendet. Versicherte, die aktuell keine durch eine PIN geschützten Anwendungen in Umgebungen des Gesundheitswesens verwenden, werden den PIN-Prozeduren nicht die notwendige Aufmerksamkeit schenken. Es kann deshalb passieren, dass dem Versicherten die PIN bei der erstmaligen Nutzung nicht mehr bekannt ist. Hier hilft die Verwendung einer Leer-PIN: bei der ersten Verwendung der Karte in der TI, die im Beisein eines Leistungserbringers erfolgen MUSS, wird die gewählte Echt-PIN eingegeben. Durch organisatorische Maßnahmen beim Leistungserbringer kann sichergestellt werden, dass nur der rechtmäßige Karteninhaber diese Umwandlung durchführt.

4.7.2 PIN.home

Durch Eingabe der PIN.home wird dem Karteninhaber der Zugriff auf seine schützenswerten Daten auf der eGK und auf die privaten Schlüssel des ENC- und AUT-Schlüsselpaares erlaubt. Bei der Erstausgabe müssen nach jetzigem Stand keine Daten auf der eGK geschützt werden; außerdem sind noch keine Anwendungen angelegt, die durch die PIN.home geschützt sind. Deshalb darf bei der Erstausgabe für die PIN.home neben dem Versand der Echt-PIN auch ein Leer-PIN-Verfahren eingesetzt werden.

Es ist möglich, bei Nutzung einer Echt-PIN die PIN.home erst später nach Anforderung durch den Versicherten, der die genannten Funktionen nutzen will, in einem PIN.Brief zu übermitteln. Dabei muss genau festgelegt werden, wie die Authentizität der Anforderung geprüft werden kann.

4.7.3 Rücksetzung der PIN

Wenn der Versicherte eine PIN dreimal falsch eingegeben hat, wird der Zugang zu den damit geschützten Anwendungen gesperrt und kann im Prinzip nur durch Eingabe der PUK wieder aktiviert werden. Dabei wird gleichzeitig die Eingabe einer neuen PIN gefordert.

4.7.3.1 Übertragung der PUK im Offline-Verfahren

Das Verfahren mit der Versendung der PUK mittels PIN/PUK-Brief im Rahmen der Kartenausgabe ist im Gesundheitswesen problematisch: Es kann nicht erwartet werden, dass der Versicherte bei jedem Besuch eines Leistungserbringers die PUK parat hat, wenn die PIN-geschützten Funktionen der Karte durch mehrfache Eingabe einer falschen PIN blockiert sind. Da zwischen Versendung des PIN-Briefes und der Notwendigkeit, die PUK zu einzusetzen, ein längerer Zeitraum liegen kann, ist der Zugriff auf den PIN-Brief möglicherweise nicht mehr möglich.

Es liegt deshalb nahe, den PUK-Brief auf Anforderung zu versenden. Zwischen der Anforderung und der Zustellung bleibt bei diesem Verfahren ein Zeitraum, in dem der Versicherte die PIN-geschützten Funktionen nicht nutzen kann.

Anhang A

A1 - Abkürzungen

Kürzel	Erläuterung
AUT	Authentisierung (Authentication)
ENC	Verschlüsselung (Encryption)
eGK	elektronische Gesundheitskarte
GVD	Geschützte Versichertendaten
HBA	Heilberufsausweis
HSM	Hardware Security Module
PIN	Personenkennung (Personal Identification Number)
PUK	Personal Unblocking Key (Resetting Code)
QES	Qualifizierte elektronische Signatur
SMC-B	Sicherheitsmodulkarte (Security Module Card) für eine Institution
VD	Versichertendaten
ZDA	Zertifizierungs-Dienste-Anbieter

A2 - Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 - Tabellenverzeichnis

A4 - Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemGesArch]	gematik (18.03.2008): Einführung der Gesundheitskarte – Gesamtarchitektur, Version 1.3.0

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemPersKrypt]	gematik (21.12.2006): Einführung der Gesundheitskarte – Personalisierung kryptographischer Daten der eGK, V1.0.0
[gemSiKo] [gemSiKo#AnhC] [gemSiKo#AnhE] [gemSiKo#AnhF]	gematik (10.03.2008): Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur Version 2.2.0, www.gematik.de Anhang C: Schutzbedarfsanalyse Anhang E: PIN/PUK-Policy Anhang F: Kryptographiekonzept
[gemSpec_eGK_P1] [gemSpec_eGK_P1#9.1.7]	gematik (20.03.2008): Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte; Teil 1: Spezifikation der elektrischen Schnittstelle Version 2.2.0, www.gematik.de Kap. PIN
[gemSpec_eGK_P2] [gemSpec_eGK_P2#6.2.7] [gemSpec_eGK_P2#6.2.8]	gematik (25.03.2008): Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte Teil 2: Grundlegende Applikationen Version 2.2.0, www.gematik.de Kap. /MF/PIN.CH Kap. /MF/PIN.home
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt