Einführung der Gesundheitskarte

Übergreifende Spezifikation CAN-Policy

|  |  |
| --- | --- |
| Version: | 1.0.0 RC |
| Revision: | \main\rel\_online\9 |
| Stand: | 30.05.2013 |
| Status: | zur Freigabe empfohlen |
| Klassifikation: | vertraulich\_LA |
| Referenzierung: | [gemSpec\_CAN\_TI] |

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich hier um eine Erstveröffentlichung

Dokumentenhistorie

| Version | Stand | Kap./ Seite | Grund der Änderung, besondere Hinweise | Bearbeitung |
| --- | --- | --- | --- | --- |
| 0.1.0 |  |  | Ersterstellung | ITS/SI |
| 0.5.0 | 24.05.13 |  | zur Abstimmung freigegeben | PL P706 |
| 1.0.0 RC | 30.05.13 |  | zur Freigabe empfohlen | PL P706 |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 5](#_Toc486508704)

[1.1 Zielsetzung 5](#_Toc486508705)

[1.2 Zielgruppe 5](#_Toc486508706)

[1.3 Geltungsbereich 5](#_Toc486508707)

[1.4 Abgrenzung 5](#_Toc486508708)

[1.5 Methodik 6](#_Toc486508709)

[2 Anforderungen an eine CAN 7](#_Toc486508710)

[3 Anhang A - Verzeichnisse 9](#_Toc486508711)

[3.1 A1 - Abkürzungen 9](#_Toc486508712)

[3.2 A2 - Glossar 9](#_Toc486508713)

[3.3 A3 - Referenzierte Dokumente 9](#_Toc486508714)

[3.3.1 A3.1 – Dokumente der gematik 9](#_Toc486508715)

[3.3.2 A3.2 – Weitere Dokumente 9](#_Toc486508716)

# Einordnung des Dokumentes

## Zielsetzung

Die übergreifende CAN-Policy gilt für Smartcards der TI, die eine kontaktlose Schnittstelle nutzen. Die Anforderungen der übergreifenden CAN-Policy stellen sicher, dass die CAN auf einem adäquaten Sicherheitsniveau geschützt wird.

## Zielgruppe

Das Dokument richtet sich an Kartenherausgeber von kontaktlosen Karten im Gesundheitswesen. Derzeit sind dies eGK und HBA. 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.

# 

# Anforderungen an eine CAN

Smartcards in der TI (eGK und HBA) können neben einer kontaktbehafteten Schnittstelle optional eine kontaktlose Schnittstelle nutzen. Soll über die kontaktlose Schnittstelle auf die Karte zugegriffen werden, ist als zusätzliche Zugriffsbedingung die Eingabe der „*Card Access Number*“ (CAN) am Kartenterminal erforderlich. Die CAN ist eine auf der Karte aufgedruckte Nummer, die auch im Chip der Karte gespeichert ist.

Die CAN wird als gemeinsames Geheimnis für den Aufbau eines kryptographisch geschützten Kanals zwischen einer kontaktlosen Smartcard und einem Kartenterminal nach dem PACE-Protokoll (Password Authenticated Connection Establishment) [ICAO-MRTD-2010] verwendet.

Die Sicherheitsziele des Kanals sind:

1. Skimming-Angriffe sollen verhindert werden. Der Besitzer der Smartcard soll durch selbstbestimmten Transfer der CAN an das Kartenterminal (entweder durch Eingabe via PIN-Pad oder durch optisches Lesen der auf der Smartcard aufgedruckten CAN durch das Kartenterminal) eine ungewollte Kommunikation der Karte mit einem Kartenterminal eines Angreifers verhindern.
2. Die Vertraulichkeit, die Authentizität und die Integrität der anschließenden Kommunikation zwischen Smartcard und Kartenterminal soll geschützt werden.

Im Folgenden werden für die CAN vom Kartenherausgeber einzuhaltende Anforderungen beschrieben. Weitere Anforderungen an die CAN der spezifischen Karte können in den Spezifikationen zu den Karten festgelegt werden.

**⌦ GS-A\_5115 Schutzbedarf der CAN**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die CAN in seinem System inklusive der Aushändigung der Karte an den Karteninhaber durch Maßnahmen und Prozesse geschützt wird, die den in Tab\_SBF\_CAN festgelegten Schutzbedarf wirksam gewährleisten.

Tabelle 1 – Tab\_SBF\_CAN, Schutzbedarfsfeststellung CAN

|  |  |  |  |
| --- | --- | --- | --- |
| **Schutzziel** | **Vertraulichkeit** | **Integrität** | **Authentizität** |
| Schutzbedarf | hoch | mittel | n.a. |

**⌫**

**⌦ GS-A\_5116 Zufällige CAN-Erzeugung**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die CAN zufällig oder pseudozufällig erzeugt wird.

**⌫**

**⌦ GS-A\_5117 Anforderungen an Zufallsgenerator für CAN-Erzeugung**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass der zur Erzeugung der CAN verwendete Zufalls- oder Pseudozufalls­ge­ne­ra­tor die vorgegebenen Mindestanforderungen der gematik entsprechend [gemSpec\_Krypt#GS-A\_4367] erfüllt.

**⌫**

**⌦ GS-A\_5118 CAN-Speicherung nur für die Personalisierung der Karte**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS die CAN aus seinen Systemen unverzüglich löschen, sobald die CAN für die Personalisierung der Karte nicht mehr erforderlich ist.

**⌫**

**⌦ GS-A\_5119 Sicherer Transport und Speicherung der CAN beim Kartenheraus­geber bzw. Kartenpersonalisierer**

Der Kartenherausgeber oder, falls der Kartenherausgeber einen Dritten mit der Kartenpersonalisierung beauftragt, der Kartenpersonalisierer MUSS sicherstellen, dass die CAN während des Transportes und der Speicherung vor nicht autorisierter Aufdeckung und Weitergabe geschützt wird.

**⌫**

**⌦ GS-A\_5120 Verteilung der CAN auf das erforderliche Maß beschränken**

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

**⌫**

**⌦ GS-A\_5121 Karteninhaber über Umgang mit CAN informieren**

Der Kartenherausgeber MUSS den Karteninhaber über den Umgang mit der CAN auf der von ihm herausgegebenen Karte informieren.

**⌫**

# 

# Anhang A - Verzeichnisse

## A1 - Abkürzungen

| Kürzel | Erläuterung |
| --- | --- |
| CAN | Card Access Number |
| eGK | elektronische Gesundheitskarte |
| HBA | (elektronischer) Heilberufsausweis |
| PACE | Password Authenticated Connection Establishment |
| TI | Telematikinfrastruktur |

## A2 - Glossar

Das Glossar 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 |
| [ICAO-MRTD-2010] | ICAO. Supplemental Access Control for Machine Readable Travel Documents, Technical Report, 2010 |