gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation eHealth-Kartenterminal

Version:	2.6.0
Stand:	26.03.2008
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Das Pairing-Verfahren (Kapitel 3.7.2) wurde überarbeitet, um einen einfachen automatisierten Austauschprozess für Konnektoren zu ermöglichen, bei dem ein neuerliches manuelles Pairing aller Kartenterminals nicht notwendig ist.

Aus den Änderungen des Pairing-Verfahrens ergeben sich auch Änderungen beim Aufbau der TLS-Verbindung (Kapitel 4.11). Das Kartenterminal muss nun prüfen, ob es sich bei dem im Rahmen des TLS-Verbindungsaufbaus präsentierten Zertifikats um ein Komponentenzertifikat eines Konnektors handelt.

Es haben sich Änderungen an den Anforderungen zum Firmwareupdate ergeben (Kapitel 3.5.13 und 3.6.3). Es ist nun zulässig eine korrekt installierte Firmware durch eine Firmware gleicher Version zu ersetzten. Eine Firmware muss korrekt in den Speicher des Terminals geschrieben worden sein bevor sie als aktive Firmware übernommen werden darf.

Es wurden weitere Details zu Festlegungen der KT-Identität und des Schlüsselmanagements (Kapitel 3.7) festgeschrieben.

Die Anforderungen an die Schlüssel, das zugehörige Zertifikat und die zulässigen Algorithmen zur Absicherung der Management-Schnittstelle wurden festgelegt.

Es wird im gesamten Dokument nun einheitlich von der Kartenterminalidentität gesprochen. Die Begriffe „Identität“, „Geräteidentität“, „Terminalidentität“ als Bezeichnung für die Kartenterminalidentität sind entfallen.

Die Länge der Displaymessage des Kommandos SICCT PERFORM VERIFICATION wurde auf 48 Zeichen angehoben.

In Fußnoten befindliche normative Aussagen wurden in den Textkörper verlagert.

Es wurden einige Fehler in der EHEALTH TERMINAL AUTHENTICATE Kommandobeschreibung (Kapitel 4.7.2) beseitigt.

Die Anforderungen an das Passwort bzw. die PIN zur Sicherung der Managementschnittstelle des Kartenterminals wurden aufgenommen.

Änderungen im Discretionary Data Data Object (Kapitel 4.7.5)

Inhaltliche Änderungen gegenüber der letzten freigegebenen Version sind gelb markiert. Sofern ganze Kapitel eingefügt oder wesentlich überarbeitet wurden, wurde zur besseren Lesbarkeit lediglich die Überschrift durch gelbe Markierung hervorgehoben.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemSpec_KT] gematik (26.03.2008): Einführung der Gesundheitskarte – Spezifikation eHealth-Kartenterminal, Version 2.6.0 www.gematik.de

Dokumentenhistorie

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	28.04.06		freigegeben	gematik
1.0.1	30.06.06		Anpassung an die SICCT-Spezifikation V1.03 sowie redaktionelle Änderungen: sichere Schlüsselspeicherung, Notwendigkeit eines Displays, gleichläufige Kartenkommunikation	gematik, AG7
1.0.3	13.07.06		Abschwächung der Forderung gleichläufiger Kartenkommunikation und Einführung einer Pflicht zur Dokumentation von Einschränkungen in diesem Bereich	gematik, AG7
1.0.4	26.07.06		Korrektur der Schlüssellängen bei TLS/AES	gematik, AG7
1.0.7	03.08.06		Einarbeitung des Dokumentes [Auth06] von TÜViT und BSI gemäß der Beschlüsse der 30ten Architekturboardsitzung. Einarbeitung eines Alternativverfahrens unter Nutzung eines Sicherheitsmoduls in Rücksprache mit BMG und TeleTrust.	gematik, AG7
1.0.8	08.08.06		Festlegung zur Sicherung des Firmware-Downloads mit asymmetrischer Kryptografie	gematik, AG7
1.1.0	09.08.06		Ersetzung der Referenz auf [Auth06] des TÜViT und BSI durch das gleich betitelte [SICCT02] mit Veröffentlichungsdatum 18.08.2006	BMG
1.2.0	23.10.06		Einarbeitung der Kommentare zu 1.1.0 Überarbeitung der Festlegungen zur Terminalidentität unter Berücksichtigung der aktuellsten Erkenntnisse aus Architekturboard und SICCT (Streichung der Referenz auf [SICCT02])	gematik
1.2.1	16.02.07		Streichung der „alphanumerischen“ Eingabemöglichkeit im Abschnitt „Benutzerführung“, da eine solche bei Nutzung eines Sicherheitsmoduls nicht notwendig ist. Erste Adaption an SICCT 1.10. Anpassung der Spezifikation für die Authentisierung beim TLS-Verbindungsaufbau für eine flexiblere Anpassung an die Einsatzumgebun-	gematik, AG7

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeitung
			gen. Einführung von einheitlichen Kommandos zur Verwaltung der Whitelist. Ergänzungen und Erweiterungen des SICCT MODIFY VERIFICATION DATA Kommandos. Festlegung zur Verbindlichkeit der in der SICCT-Spezifikation definierten Betriebsmodi „BCS“ und „SICCT“.	
1.2.2	25.02.07		Einarbeitung der Reviewergebnisse aus der internen QS	gematik, AG7
1.3.0	02.03.07		freigegeben	gematik
1.3.1	22.04.07		Aufnahme des Pairings von KT und Konnektor Spezifikation der SM-KT Berücksichtigung der Einsatzumgebung des KT Festlegung des Display-Größe Setzen der Whitelist auf optional, als Modus beim Aufbau der TLS-Verbindung Einarbeitungen von Kommentierungen	gematik, AG7
1.3.3	23.04.07		Format-Korrekturen Überarbeitung des Abschnitts SM-KT Einbringung der Referenzen auf [gemSpecKrypt] unter Entfernung konkreter Algorithmen und Schlüssellängenvorgaben.	gematik, AG7
1.3.7	04.05.07		Einarbeitungen von Reviewergebnissen	gematik, AG7
2.0.0	04.05.07		freigegeben	gematik
2.0.1	19.07.07		Einarbeitung von Reviewergebnissen	gematik, AG7
2.0.2	26.07.07		Einarbeitung von Reviewergebnissen. Entfernen der Erweiterungen zum NULL-PIN Verfahren. Vervollständigung der offenen Punkte. Referenzierung auf SICCT 1.20 geändert.	gematik AG7
2.1.0	02.08.07		nicht freigegeben	gematik
2.1.2	21.8.07		Änderungen, die sich aus der Entscheidung ergeben, dass die Bauart nicht mehr auf der SM-KT gespeichert wird	gematik AG7
2.2.0	24.08.07		freigegeben	gematik
2.2.1	11.10.07		Einarbeitung von Reviewergebnissen sowie den Festlegungen der Kartenterminalidentität und den Ergebnissen des SICCT WS vom 13.9.2007	gematik AG7
2.2.2	16.10.07		Präzisierung der normativen Formulierungen	gematik AG7

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeitung
2.2.3	24.10.07		Einarbeiten von Reviewergebnissen	gematik AG7
2.2.6	29.10.07		Überarbeitung der Kapitelreferenzen	gematik AG7
2.2.9	19.11.07		Einarbeiten von Reviewergebnissen Verlagerung von Kap 4.12 in 3.7	SPE/DK
2.3.1	05.12.07		Kapitel 3.7.3 entfernt	SPE/DK
2.3.2	06.12.07		Anpassen der SICCT Kapitelreferenzen, redaktionelle Änderungen.	SPE/DK
2.4.0	06.12.07		freigegeben	gematik
2.4.1	21.12.07		Korrektur der Längenangaben einiger E-HEALTH Befehlen	SPE/DK
2.4.3	22.01.08		Einarbeiten von Reviewergebnissen	SPE/DK
2.4.4	24.01.08		Einarbeiten des neuen Pairingprozesses und daraus resultierender Änderungen im Rahmen des TLS-Verbindungsaufbaus	SPE/DK
2.4.8	11.02.08		Einarbeiten von Reviewergebnissen	SPE/DK
2.4.9	12.02.08		Redaktionelle Überarbeitungen	SPE/DK
2.5.0	15.02.08		freigegeben	gematik
2.5.1	26.03.08		Einarbeiten von externen Reviewergebnissen	SPE/DK
2.5.2	26.03.08		Änderungen im Discretionary Data Data Object	SPE/DK
2.6.0	26.03.08		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Kartenterminals für Anwendungen im Gesundheitswesen MÜSSEN einer Vielzahl von Anforderungen genügen:

- Sicherheitstechnische Anforderungen ergeben sich aus der Nutzung im Rahmen der Erzeugung qualifizierter Signaturen[1] und aus der Verarbeitung und Speicherung personenbezogener Daten auf Karten. Die Bedingungen des Signaturgesetzes und der Signaturverordnung MÜSSEN erfüllt sein, um die Terminals im Rahmen einer Signaturumgebung zu nutzen.
- Eine leichte Integrierbarkeit der Kartenterminals in bestehende Umgebungen und interoperable Austauschbarkeit in zukünftig etablierten Umgebungen stellen eine langfristige Wartbarkeit der dezentralen Infrastruktur sicher. Es wird so sichergestellt, dass nach Auswahl eines Kartenterminals die Wahlfreiheit beim Einsatz von Primärsystemen oder Konnektoren erhalten bleibt.
- Die Kompatibilität zu den Gesundheitskarten eGK und HBA und die fehlerfreie Kommunikation mit diesen erfordert, dass die Kartenterminals für den Betrieb mit Chipkarten gemäß den ISO-Normen ausgelegt sind. Darüber hinaus ist ein Lesen der KVK für eine reibungslose Migration erforderlich.
- Aus den Geschäftsprozessen eines Leistungserbringers entstehen Anforderungen an die Funktionalität des Terminals: dies betrifft vor allem eine aktive, zeitnahe Rückmeldung über Ereignisse an die ansteuernden Komponente(n) aber auch die Anzeige von Nachrichten zur Benutzerführung.
- Die Verwendung der Kartenterminals im Rahmen der Telematik im Gesundheitswesen unterscheidet sich von anderen Kartenanwendungen durch die Anbindung des Kartenterminals über ein Local Area Network (LAN) an die ansteuernden Komponenten. Durch die entstehende Kommunikationsmöglichkeit zwischen einem Kartenterminal und vielen Computersystemen werden zusätzliche Mechanismen für die sichere Identifikation und Authentisierung eines betriebszugelassenen Kartenterminals benötigt. In diesen Rahmen fällt auch das automatische Auffinden von verfügbaren Chipkartenterminals durch den Konnektor.

Hieraus ergeben sich zusätzliche Anforderungen an ein Kartenterminal, die über die SICCT-Spezifikation hinausgehen und speziell für das Gesundheitswesen Anwendung finden. Die hier formulierten Anforderungen erweitern oder konkretisieren die SICCT-Spezifikation, so dass ein Höchstmaß an Interoperabilität sichergestellt wird. Hervorzuheben ist, dass die Kernfunktionalität der Kartenterminals, unabhängig vom jeweiligen Einsatzgebiet, immer gleich bleibt: eine performante, fehlerfreie Kommunikation zur Chipkarte MUSS ermöglicht werden und die notwendigen Sicherheitsfunktionalitäten MÜSSEN abgebildet sein. Darüber hinaus bleibt den verschiedenen Herstellern die Möglichkeit mit zusätzlichen Komfortcharakteristiken differenzierende Faktoren zu schaffen.

[1] Qualifizierte Signaturen sind in der Telematikinfrastruktur z. B. für Verordnungsdaten vorgesehen und werden unter Nutzung von elektronischen Heilberufsausweisen (HBA) erzeugt.

Die in dieser Spezifikation beschriebenen Anforderungen an ein Chipkartenterminal sind für eine Netzwerkumgebung spezifiziert. Kompatibilität zu den eingesetzten Karten und Offenheit für zukünftige Anwendungen im Gesundheitswesen stehen im Fokus.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Um die Interoperabilität zwischen den verschiedenen Komponenten innerhalb der Telematikinfrastrutur im Gesundheitswesen sicherzustellen und alle funktionalen und nichtfunktionalen Anforderungen abzubilden, spezifiziert dieses Dokument die im Gesundheitswesen — in Verbindung mit der elektronischen Gesundheitskarte — einzusetzenden Kartenterminals.

Als Grundlage dieser Spezifikation gilt die SICCT-Spezifikation (Secure Interoperable Chip-Card Terminal) [SICCT] der TeleTrusT. Darauf aufbauend werden die speziellen und abweichenden Anforderungen des Gesundheitswesens beschrieben.

Relativ zur SICCT-Spezifikation werden sowohl neue Anforderungen eingeführt als auch Forderungen der SICCT-Spezifikation außer Kraft gesetzt.

2.2 Zielgruppe

Das Dokument wendet sich an die Hersteller von Kartenterminals für den Einsatz im Deutschen Gesundheitswesen, an die Hersteller von eHealth-Konnektoren und an die zuständigen Prüf- und Zulassungsstellen, sowie an die Leistungserbringer mit ihren Administratoren und die Primärsystemhersteller mit ihren Servicekräften.

2.3 Geltungsbereich

Die hier getroffenen Festlegungen sind für den Einsatz von Kartenterminals sowie angrenzender Systeme, welche über die hier definierten Schnittstellen mit dem Kartenterminal interagieren, in der Telematikinfrastruktur des deutschen Gesundheitswesens verbindlich.

2.4 Arbeitsgrundlagen

Grundlage für die Spezifikation sind die §§ 291 und 291a des SGB V, SigG und SigV sowie die Rechtsverordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte.

Das Kartenterminal basiert auf der Spezifikation SICCT, welche durch additive und subtraktive Vorgaben für den Betrieb als eHealth-Kartenterminal in diesem Dokument eingeschränkt und erweitert wird. Kartenterminals für den Einsatz in der Telematikinfrastruktur des deutschen Gesundheitswesens MÜSSEN sich konform zu diesem Dokument und den durch dieses Dokument referenzierten Spezifikationen verhalten.

2.5 Abgrenzung des Dokumentes

Für globale Anforderungen an multifunktionale Kartenterminals wird auf die Spezifikation „SICCT Secure Interoperable ChipCard Terminal“ [SICCT] verwiesen. Für spezielle Anforderungen gilt dieses Dokument.

Die SICCT-Spezifikation dient dabei als Basisdokument und

- orientiert sich an frei verfügbaren internationalen Standards,
- beschreibt technische Spezifikationen der Kommunikationsebene(n) und
- beschreibt grundlegende Sicherheitsanforderungen.

Dieses Zusatzdokument

- beschreibt besondere funktionelle Anforderungen an ein eHealth-Kartenterminal,
- gibt besondere sicherheitstechnische Anforderungen vor und
- beschreibt technisch notwendige Maßnahmen für eine gleichzeitige Nutzung von bestehenden Systemen basierend auf der Krankenversichertenkarte (KVK) und neuen Diensten der Telematikinfrastruktur für das Gesundheitswesen auf Basis der eGK während einer befristeten Übergangszeit (Migration).

2.6 Methodik

2.6.1 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 dringende Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **SOLL NICHT** kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **KANN** bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

2.6.2 Normative und informative Kapitel

Kapitel mit normativen Inhalten tragen hinter der Kapitelüberschrift den Hinweis:

(normativ)

Modellartefakte sind normativ, wenn sie nicht explizit als informativ gekennzeichnet werden.

Auf Abschnitte mit rein informativen Inhalten (Systemüberblick, Grundlagen, alternative Betrachtungen) wird im Text hingewiesen.

Nachverfolgbarkeit von Anforderungen: Enthält ein Satz ein RFC-Schlüsselwort (MUSS, DARF NICHT, etc.) muss am Ende des Satzes die hier spezifizierte Ausgangs-Anforderung durch ihre ID in eckigen Klammern referenziert werden. Besteht die Anforderung aus mehr als einem Satz, muss jeder weitere Satz ein RFC-Schlüsselwort der gleichen RFC-Kategorie enthalten.

Werden Eingangsanforderungen durch Modellartefakte realisiert, müssen die Modellartefakte eindeutig referenziert werden.

Lassen sich aus Modellartefakten Ausgangsanforderungen ableiten, sind das neue Anforderungen.

2.6.3 Hinweis auf offene Punkte

Auf offene Punkte wird durch einen Text in nachfolgendem Format hingewiesen:

Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

3 Architektur (normativ)

3.1 Anschlussarten eines Terminals

Die konkrete Ausprägung (d. h. Bauform) eines Kartenterminals für den Einsatz im Rahmen der Telematikinfrastruktur im Gesundheitswesen wird durch diese Spezifikation nicht vorgegeben, sondern nur die funktionalen und nicht-funktionalen Anforderungen. Grundsätzlich kennt die Architektur der Telematikinfrastruktur im Gesundheitswesen nur netzwerkfähige Kartenterminals, jedoch sind auch Mischformen vorstellbar. Die jeweilige Ausprägung wird primär von den Anforderungen der Geschäftsprozesse und den Sicherheitsanforderungen vorgegeben.

Zur Erläuterung ist anzumerken, dass zwei grundsätzlich unterschiedliche Lösungsansätze zur Realisierung der Anforderungen dieser Spezifikation möglich sind:

- **Netzwerkfähige Kartenterminals** werden über eine TLS-Verbindung angesteuert. Die TLS-Verbindung terminiert im Kartenterminal und sichert die Kommunikation mit dem Kartenterminal ab. Die Ausprägung des Netzwerks zwischen Kartenterminal und Konnektor wird hier nicht betrachtet. Für die Zulassung durch die gematik MUSS ein netzwerkfähiges Kartenterminal mittelbar oder unmittelbar über eine Ethernet-Verbindung angesteuert werden können. Falls ein netzwerkfähiges Kartenterminal nur mittelbar über Ethernet angesteuert werden kann, ist der gematik ggf. technischer Support zu leisten. Die vorliegende Spezifikation ist in diesen Fällen direkt vom Kartenterminal zu erfüllen und nur das Kartenterminal stellt einen Prüf- und Evaluationsgegenstand[2] dar.

- **Virtuelle Kartenterminals** entstehen durch die Kombination einer Software mit einem nicht-netzwerkfähigen Kartenterminal (z.B. mit einer seriellen Schnittstelle) oder einem netzwerkfähigen Kartenterminal, welches nicht die hier gestellten Schnittstellenanforderungen erfüllt. Die adaptierende Software läuft dabei auf einem anderen Gerät ab und „exportiert“ das Kartenterminal mit den Schnittstellen und Funktionalitäten wie in dieser Spezifikation beschrieben. Die Verbindung zwischen Kartenterminal und adaptierendem Gerät muss dabei entweder durch den Nutzer des Kartenterminals überschaubar oder der Datenfluss zwischen Kartenterminals und Adapter verschlüsselt sein. Bei diesem Vorgehen sind die Softwarekomponente, deren Ausführungsumgebung, die Verbindung zwischen dem Kartenterminal und der Ausführungsumgebung und der Schlüsselspeicher der Ausführungsumgebung Bestandteil des zu prüfenden und zu evaluierenden Gegenstands[2].

Grundsätzlich gelten dieselben Zulassungsrichtlinien für virtuelle und netzwerkfähige Kartenterminals.

[2] Prüf- und Evaluierungsgegenstand im Sinne einer Sicherheitszertifizierung und der Zulassung durch die gematik gemäß [gemZulKomp-KT].

3.2 Gesetzliche Anforderungen

Bei der Konzeption des eHealth-Kartenterminals ergeben sich zusätzliche Anforderungen sowohl aus dem Bundesdatenschutzgesetz (BDSG) als auch aus dem Signaturgesetz. Das Bundesdatenschutzgesetz regelt die bei der Verarbeitung und Speicherung personenbezogener Daten (Patienten- bzw. Versichertendaten) einzuhaltenden technischen und organisatorischen Maßnahmen, die zum Schutz der betreffenden Daten gemäß §9 Satz 1 BDSG und Anlage zu §9 Satz1 BDSG zu treffen sind.

Das Signaturgesetz [SigG01] definiert die gesetzlichen Vorschriften bzgl. der digitalen Signatur. Von besonderem Interesse ist hier §17 *Produkte für qualifizierte elektronische Signaturen*. Weiterführende Vorschriften finden sich dazu auch in der Signaturverordnung [SigV01].

3.3 Zulassungsverfahren, Zertifikat

Für eine Zulassung des eHealth-Kartenterminals sind sicherheitstechnische und funktionale Prüfungen erforderlich. Das Zulassungsverfahren unterliegt den Vorgaben und der Aufsicht der *gematik*. Die Erteilung einer Zulassung erfolgt durch die *gematik* oder von ihr bevollmächtigte Dritte, siehe auch [gemZulKomp-KT].

Eine durch die *gematik* akkreditierte Prüfstelle konzentriert Herstellererklärungen, Nachweise und Teilzertifikate, bewertet die Eignung, erstellt einen zusammenfassenden Bericht und reicht diesen an die Zulassungsstelle weiter, welche die Vollständigkeit und Korrektheit überprüft und einen abschließenden Interoperabilitätstest durchführt.

3.4 Zulassungsanforderungen

Die notwendigen Teilprüfungen und Teilzertifikate sind der gesonderten Dokumentation des Zulassungsverfahrens der *gematik* zu entnehmen (s. [gemPKI_KT]). Insbesondere benötigt das eHealth-Kartenterminal eine sicherheitstechnische Qualifikation in Form einer Sicherheitszertifizierung und einer Betriebszulassung durch die *gematik*.

Grundfunktionen, insbesondere als Teil der Signaturanwendungskomponente werden aufgrund eines Protection Profiles (s. 3.6.8) evaluiert. Ein ergänzendes Sicherheitsgutachten oder eine erweiterte Evaluierung bestätigt die Kontinuität der Sicherheitsmechanismen bei individuellen Ergänzungen und Produktausprägungen und die berücksichtigten Aspekte des Datenschutzes.

Bei Kartenterminals, die diese Spezifikation mit zusätzlichen Funktionalitäten erweitern, MUSS nachgewiesen werden, dass diese Zusatzfunktionen keine Sicherheitsziele des Schutzprofils nachteilig beeinflussen.

3.5 Allgemeine Anforderungen

In den folgenden Kapiteln sind die zu erfüllenden funktionalen und nicht-funktionalen Anforderungen an das eHealth-Kartenterminal aufgelistet und gleichzeitig Voraussetzungen an die beteiligten dezentralen Systemkomponenten bei den Leistungserbringern beschrieben.

3.5.1 Integration

Die Integration und Ansteuerung des eHealth-Kartenterminals erfolgt über einen Konnektor.

3.5.2 Migrationsfähigkeit

Das eHealth-Kartenterminal MUSS sich für eine Migration von der Krankenversichertenkarte [KVK] zur eGK [gemSpec_eGK_P2] eignen.

Das bedeutet, dass die technische Funktionalität den Betrieb von kontaktbehafteten Speicher- wie auch Prozessorkarten erlaubt, und die Geräte konzeptionell für folgende Einsatzszenarien verwendbar sein MÜSSEN:

- Verarbeitung spezifikations- und norm-konformer KVKs,
- Verarbeitung spezifikations- und norm-konformer eGKs,
- Verarbeitung von Daten (Lesen) vom Medium KVK,
- Verarbeitung von Daten (Lesen und Schreiben) vom Medium eGK.

3.5.3 Signaturanwendungskomponente

Das eHealth-Kartenterminal MUSS sich in Verbindung mit der entsprechenden Software des Konnektors als Teil einer Signaturanwendungskomponente (HW und SW) entsprechend der Anforderungen aus SigG [SigG01] und SigV [SigV01] zur Erstellung von qualifizierten elektronischen Signaturen eignen.

3.5.4 Anforderungen an die Kartenterminals

eHealth-Kartenterminals MÜSSEN aus Gesamtsystemsicht folgende Funktionen einem Konnektor bereitstellen:

- einen Zugriff auf einen oder mehrere Kartensteckplätze und darin gesteckte Chipkarten,
- eine eindeutige Adressierbarkeit jedes Kartenslots,
- eine Koordination der Zugriffe auf die Karten bzw. Exklusivität des Zugriffs,
- Information über bestimmte Ereignisse (z. B. »Karte wurde (in zeitlicher Nähe) gesteckt«) und einen Eventmechanismus zur Meldung an den Konnektor (zur Vermeidung von Polling),
- eine authentisierte, verschlüsselte und integritätsgesicherte Kommunikation,
- eine eindeutige, kryptographische Identität in einem „sicheren“ Schlüsselspeicher, für den gilt, dass die Schlüssel NICHT durch einen Angreifer aus dem Gerät auslesbar sein DÜRFEN. Da die kryptographische Identität die Kommunikation von der Signaturanwendungskomponente auf dem Konnektor zum Kartenterminal sichert, MUSS hier gegen ein hohes Angriffspotential gesichert werden.

3.5.5 Benutzerführung

Zur Benutzerführung ist ein integriertes Display erforderlich. Das Display MUSS mindestens zwei Zeilen à 16 Zeichen als ASCII-Text darstellen können. Die Fähigkeit zur Anzeige von weiteren Sonderzeichen und Symbolen ist erlaubt. Graphische Displays, die in der Lage sind die zwei Zeilen anzuzeigen, sind zugelassen.

Zur Eingabe einer PIN und zur damit verbundenen Authentisierung des Nutzers MUSS ein Tastenfeld oder eine vergleichbare Eingabemöglichkeit für eine numerische PIN vorgesehen sein. Weitere Sensoren/Eingabeeinheiten KÖNNEN im Kartenterminal vorgesehen sein.

Bei einem „virtuellen Kartenterminal“ KANN die Benutzerführung auch über eine externe Anzeigeeinheit realisiert sein; diese unterliegt hier auch denselben Anforderungen einer Sicherheitsprüfung und -zulassung.

3.5.6 Performanz

Das eHealth-Kartenterminal SOLL in seiner Konstruktion und Programmierung derart ausgelegt sein, dass es die Übertragungsraten zum Hostsystem und zu den Chipkarten, entsprechend den technischen Spezifikationen[3], unterstützt: interne Abläufe des Kartenterminals DÜRFEN NICHT die Kommunikation zu externen Einheiten verzögern. Speziell ist die gleichzeitige Kommunikation mit einem HBA und einer eGK oder einer SMC-A und einem HBA oder eGK zu betrachten. Solch gleichzeitige Kartenkommunikation kann mehreren Transaktionen zuzurechnen sein und SOLL daher gleichläufig abgearbeitet werden. Bzgl. der Geschwindigkeit für die Kommunikation zwischen Kartenterminal und Karte ist hier Kap. 4.2.2 zu beachten.

3.5.7 Zuverlässigkeit

Zuverlässigkeitsaspekte sind ein Differenzierungsmerkmal verschiedener Produkte und Hersteller. Durch die hohe Anzahl von Steckzyklen und die häufige Nutzung unterliegen die Kartenterminals im Gesundheitssystem anderen Beanspruchungen als Consumer-Geräte. Dies ist zu berücksichtigen. Eine Haltbarkeit im Betrieb (im Sinne der MTBF bei rund-um-die-Uhr Betrieb) von mindestens 3 Jahren bzw. 200.000 Steckzyklen MUSS gewährleistet werden.

Es ist eine Zuverlässigkeitsprognose des Liefergegenstandes mit Darstellung der zugrunde gelegten Ausfallraten und Stückzahlen der Bauelemente und der anderen zuverlässigkeitsrelevanten Elemente (Lötstellen, Leiterbahnen, etc.) bereitzustellen. Die Prognose ist nachvollziehbar darzustellen, Schätzungen sind zu erläutern.

3.5.8 Stromversorgung

Die Belastbarkeit des Netzteils des eHealth-Kartenterminals MUSS so beschaffen sein, dass ein Dauerbetrieb des Chipkartenterminals von 24 Stunden pro Tag möglich ist, ohne dass eine Einschränkung der Funktionsfähigkeit zu verzeichnen ist[4].

Dies schließt mit ein, dass eine dauerhafte Stromversorgung der Chipkarte(n) mit dem Maximalstrom nach den derzeit gültigen internationalen Standards ([ISO7816-3] und [EMV_41])

[3] Technische Spezifikationen im Sinne von [SICCT], [gemSpec_eGK_P2], [HPC-P1]

[4] Zum Nachweis der Belastbarkeit im Dauerbetrieb sind Berechnungen zulässig.

gewährleistet sein MUSS[5]. Dabei ist zu beachten, dass Chipkarten kurzzeitig auch einen höheren Strombedarf haben können. In jedem Fall MUSS auch hier die volle Funktionsfähigkeit des Chipkartenterminals gewährleistet sein.

3.5.9 Fehlertoleranz

Das eHealth-Kartenterminal MUSS transiente bzw. überbrückbare Fehlerzustände bei der Kartenkommunikation erkennen und automatisch bereinigen; konkret bezieht sich dies auf die Resynchronisation der Kartenkommunikation.

Bedienungsfehler und ungültige Eingaben sind am Display (gemäß 3.5.5) zu signalisieren.

3.5.10 Wartbarkeit

Das eHealth-Kartenterminal erlaubt einen bis auf das Einspielen von Firmwareupdates wartungsfreien Betrieb. Besondere Anforderungen der Zulassung (Sicherheitssiegel) erlauben keine Öffnung des Gerätes zu Wartungszwecken. Grundsätzlich DARF es NICHT möglich sein, vom Gehäuse solche Klappen zu öffnen bzw. Abdeckungen zu entfernen, die einen Zugang zu sicherheitskritischen Bauelementen des Terminals gewähren, ohne dass ein Gerätesiegel zerstört wird.

3.5.11 Gehäuse

Die genauen Anforderungen an das gematik Prüfzeichen, z. B. ob es aufgeklebt, gedruckt oder geprägt sein muss, sind noch nicht spezifiziert.

Die MAC-Adresse des Kartenterminals MUSS am Kartenterminal erkennbar sein. Hierzu sind zwei Mechanismen zulässig. Entweder sie ist gut erkennbar auf dem Gehäuse aufgebracht (auf ein geklebtes Label gedruckt oder direkt aufgedruckt sowie geprägt) oder die MAC-Adresse ist über eine lokale Terminalfunktion abrufbar (z. B. auf dem Display). Diese Funktion MUSS immer verfügbar sein, insbesondere auch ohne LAN-Verbindung. Es DARF NICHT erforderlich sein, sich am Kartenterminal zu authentifizieren, um die MAC-Adresse über die lokale Terminalfunktion abzufragen.

Das gematik Prüfzeichen MUSS gut erkennbar auf dem Gehäuse aufgedruckt oder eingeprägt sein. Das Gehäuse MUSS Platz für ein gematik Prüfzeichen an einer für den Benutzer gut sichtbaren Stelle bieten. Die Berechtigung zur Nutzung des Prüfzeichens durch den Hersteller erfolgt mit der Zulassung der Geräte durch die gematik.

3.5.12 Kommunikationsprotokolle

Aus Gründen der Interoperabilität ist ein einheitliches Übertragungsprotokoll zum Konnektor erforderlich.

Hierzu wird in der SICCT-Spezifikation und der Konnektor-Spezifikation [gemSpec_Kon] eine einheitliche und standardisierte Benutzung des TCP/IP Protokolls beschrieben.

[5] Durch diese Anforderung soll vor allem sichergestellt werden, dass ein Kartenterminal während seines Betriebs jederzeit über eine ausreichende Stromversorgung für den Betrieb der Chipkarten verfügt.

3.5.13 Firmware-Update

Das Kartenterminal verfügt über eine sichere Updatemöglichkeit der KT-Firmware. Die sicherheitstechnischen Anforderungen an das Firmwareupdate sind Kapitel 3.6.3 zu entnehmen.

Das Update erlaubt:

- Austausch der kompletten Firmware,
- Fehlerkorrektur (Patches),
- Erweiterung/Änderung der Funktionalitäten im Rahmen der physikalischen Ausprägungen,
- Erweiterung/Änderung des Kommandosatzes,
- Erweiterung/Änderung der Chipkartenprotokolle im Rahmen der physikalischen Möglichkeiten,
- Erweiterung/Änderung der Schnittstellenübertragungsprotokolle im Rahmen der physikalischen Möglichkeiten.

3.5.14 Terminal Managementverfahren

Das Kartenterminal verfügt über Funktionalitäten, um über das Netzwerk administriert werden zu können. Diese Schnittstelle KANN sowohl vom Konnektor, von Administrationsprogrammen der Hersteller als auch über das Webinterface durch den Administrator bedient werden. Es MUSS zusätzlich sichergestellt sein, dass Änderungen nur von berechtigten Akteuren durchgeführt werden können. Vor der Anzeige von sicherheitsrelevanten Konfigurationsdaten MUSS eine Authentifizierung stattfinden. Die Verbindung zu den Netzwerkbasierten Managementschnittstellen MUSS immer mindestens mit TLS 1.0 gemäß [RFC2246] gesichert sein. Zusätzlich SOLL sie auch mittels TLS 1.1 gemäß [RFC4346] gesichert werden können. In TLS Extension [RFC3546] beschriebene funktionale Erweiterungen MÜSSEN umgesetzt werden[6].

Die Managementfunktionen, die nicht sicherheitsrelevant sind, umfassen:

- Anzeigen der aktuellen Netzwerkkonfiguration,
- Ändern der Netzwerkkonfiguration,
- Verwendung von DHCP oder statischer Konfiguration,
- Standard IP Adresse, Netzwerkmaske, Gateway,
- DNS-Server-Adresse(n),
- DNS-Name des Terminals.

[6]Ein mit dem Schlüsselwort „MUSS“ gekennzeichneter RFC ist verpflichtend in dem Sinne, dass die normativen Vorgaben dieses RFC gemäß RFC2119 Gültigkeit haben. Der [RFC3546] zu TLS-Extensions gibt nicht normativ vor, dass die TLS-Extensions unterstützt werden müssen, sondern nur, wie sie ggf. umzusetzen sind. Daher ist keine der Anforderungen des [RFC3546] verpflichtend umzusetzen, werden sie umgesetzt, sie sind jedoch RFC-konform umzusetzten.

Für die folgenden sicherheitsrelevanten Managementfunktionen KANN es notwendig sein, dass aus Sicherheitsgründen im Protection Profile des Kartenterminals Eingaben am Pinpad des Kartenterminals vorgeschrieben werden:

- Zertifikate/Schlüssel Informationen anzeigen,
- Management der am Terminal verfügbaren Karten-Slots,
- Vergabe logischer Namen,
- Firmware Update,
- Zurücksetzen der Konfiguration in den Werkszustand.

3.5.15 Mehrwertdienste

Anforderungen und Details zu den Mehrwertdiensten werden erst in Release 3 betrachtet..

Mehrwertdienste des Kartenterminals (MWD) sollen es ermöglichen zusätzliche Anwendungen mit eGK/HBA oder anderen Chipkarten, in einem eHealth-Kartenterminal zu ermöglichen. Es muss zwischen den hier benannten Mehrwertdiensten der Kartenterminals und jenen der TI, die über einen Konnektor angeboten werden, unterschieden werden. Letztere sind nicht Bestandteile der folgenden Betrachtungen.

Die gleichzeitige Verwendung von eHealth-Applikationen und herstellerspezifischen Mehrwertdiensten kann ein Sicherheitsrisiko darstellen. Um die Sicherheit bei gleichzeitiger Verwendung von MWD und eHealth-Applikationen sicher zu stellen, müssen alle Mehrwertdienste von der gematik zugelassen werden.

Mehrwertdienste müssen den Sicherheitsanforderungen der gematik genügen. Sie dürfen keine Störungen der eHealth-Anwendungen verursachen und dürfen nicht auf Bereiche der eHealth-Anwendungen zugreifen, dies schließt auch eHealth-Anwendungen auf der eGK und dem HBA mit ein.

Hierzu müssen pro Mehrwertdienst die von der gematik vorgegebene Sicherheitsdokumente und gegebenenfalls -nachweise vorgelegt werden. Die Zulassung wird einzeln je beantragten Mehrwertdienst entschieden. Ein Kartenterminal wird immer gesamt durch die gematik freigegeben, also immer inklusive einer Prüfung aller darauf laufenden Mehrwertanwendungen. Eine zusätzliche Mehrwertanwendung DARF NICHT ohne vorherige Freigabe durch die gematik nachgeladen werden.

3.5.16 Zugriffsanzeige

Das Kartenterminal MUSS Kartenzugriffe (Lesen, Schreiben, Operationsausübung) auf Chipkarten im ID-1 Format für den Benutzer gut sichtbar anzeigen, z. B. mittels einer LED die bei Kartenzugriff blinkt. Es ist weder erforderlich, Zugriffe für jede Karte separat noch die Art des Zugriffs anzuzeigen. Es MUSS lediglich der Umstand anzeigt werden, dass auf eine Karte im Kartenterminal zugegriffen wird und dies für die gesamte Dauer des Zugriffs.

3.6 Spezielle sicherheitstechnische Anforderungen

Basissicherheitsanforderungen sind im Kapitel 8 der SICCT-Spezifikation [SICCT] beschrieben. Weitere Sicherheitsanforderungen ergeben sich aus den Anforderungen des §15 ff. der Signaturverordnung [SigV01] in Relation zum §17 des Signaturgesetzes [SigG01] an Signaturanwendungskomponenten.

Eine Verifikation oder Verarbeitung der Daten einer KVK im eHealth-Kartenterminal ist nicht vorzusehen. Es erfolgt lediglich ein lesender Zugriff auf die KVK: die KVK wird vom eHealth-Kartenterminal als Speicherkarte behandelt. Darauf aufbauende Plausibilitätsprüfungen sind nur im Zusammenspiel mit dem Konnektor umzusetzen. Da keine Erkennung einer KVK als spezielle Karte vorzusehen ist und eine solche nur als Speicherkarte erkannt werden braucht, ist auch ein Schreibschutz nur in Kombination mit einem Konnektor möglich.

3.6.1 Sicherer Kanal

Terminalkommandos sowie die Kommunikation zu Managementschnittstellen MÜSSEN zwischen Konnektor und eHealth-Kartenterminal immer über verschlüsselte Netzwerkverbindungen ablaufen, wobei es dem Kartenterminal freisteht auch unverschlüsselten Zugriff für andere Anwendungen auf anderen Ports oder lokalen Anschlüssen anzubieten.

Die Kommandos zum Auffinden der Terminals (Service Discovery) benötigen keine verschlüsselten Verbindungen.

3.6.2 Benutzeridentifikation und -authentifizierung

Um auf gesicherte Kartenbereiche zugreifen oder geschützte Kartenapplikationen nutzen zu können, ist eine Identifikation und Authentifizierung des berechtigten Nutzers erforderlich.

3.6.3 Firmware-Update

Das eHealth-Kartenterminal verfügt über eine gesicherte Updatemöglichkeit der KT-Firmware.

Das Kartenterminal erkennt hierbei selbständig Übertragungsfehler und nicht authentische Übertragungen. Das hierzu notwendige Sicherheitsattribut liegt in einem auslesegeschützten Bereich des Terminals. Das Verwaltungsverfahren entspricht mindestens den Anforderungen, die in der Sicherheitsevaluierung und dem zugehörigen Protection Profile sowie den Sicherheitszielen zu Grunde gelegt werden.

Es MUSS sichergestellt sein, dass ein Austausch der Firmware nur gegen höhere Versionen als installiert möglich ist[7], und nur nach Prüfung der Integrität und Authentizität der Firmware (siehe [gemSiKo#B4.2.4]). Ist im Sinne einer entdeckten Regression ein Rückfall auf einen älteren Versionsstand notwendig, so MUSS ein solcher mit einer neuen Versionsnummer versehen werden. Das neuerliche Einspielen einer bereits installierten Firmware mit derselben Version KANN möglich sein, es MUSS jedoch sichergestellt sein, dass die aktuell instal-

[7] Die Einschränkung des Upgrades „nur auf aktuellere“ Versionsstände dient dazu, dass ein Nutzer nicht gezielt auf ältere Versionsstände zurückfallen kann, die potentiell bekannte Sicherheitslücken enthalten.

lierte Firmware korrekt installiert ist. Die Art der Versionierung (d. h. ob über Versionsnummern oder ein Veröffentlichungsdatum) bleibt herstellerspezifisch.

Bei einer fehlerhaften oder nicht authentischen Übertragung werden der Download abgewiesen und keinerlei Veränderungen an der zertifizierten Softwareversion vorgenommen. Es MUSS sichergestellt sein, dass das eHealth-Kartenterminal die Firmware nur dann als aktive Firmware übernimmt, nachdem sie vollständig und korrekt in den Speicher übernommen wurde.

Eine Veränderung der Firmware ist der Zulassungsstelle schriftlich anzuzeigen. Die Veränderungen der Firmware werden bewertet; bei Bedarf werden Zusatzprüfungen durchgeführt. Die Zulassung wird erneuert.

3.6.4 Anzeige des vertrauenswürdigen Zustands

Die genauen Anforderungen an die Mehrwertdienste, sowie die dadurch nötigen Sicherheitsmassnahmen befinden sich noch in Abstimmung.

Im vertrauenswürdigen Zustand befindet sich das eHealth-Kartenterminal in einem Modus, bei dem keine Beeinflussung und keine Informationsabschöpfung durch Komponenten (dazu zählt auch Software) welche nicht über eine Zulassung durch die gematik verfügen möglich ist.

Das Kartenterminal MUSS sicherstellen, dass SICCT- bzw. EHEALTH-Kommandos ausschließlich im vertrauenswürdigen Zustand ausgeführt werden. Daher braucht der vertrauenswürdige Zustand nicht zwingend angezeigt werden. Wird der vertrauenswürdige Zustand nicht am Gerät angezeigt, so MUSS in der Benutzerdokumentation allgemeinverständlich beschrieben werden, dass das Kartenterminal sicherheitsrelevante SICCT- bzw. EHEALTH-Befehle ausschließlich in einem vertrauenswürdigen Modus ausführt.

Da Mehrwertdienste durch die gematik zugelassen sind (siehe Kapitel 3.5.15), gibt es keine gegenseitige Beeinflussung. Daher bleibt der vertrauenswürdige Zustand auch während der Ausführung von Mehrwertdiensten erhalten.

3.6.5 Sicherer PIN-Modus

Der sichere PIN-Modus besagt, dass Pin-Eingaben am Kartenterminal nicht in die unsichere Umgebung des Personalcomputers oder über offene Übertragungswege an den Client gelangen.

Es MUSS erkennbar sein, ob sich das Kartenterminal in einem sicheren PIN-Modus befindet, um den Schutz von am Pin-Pad eingegebenen, geheim zu haltenden Daten (z. B. PIN) gewährleisten zu können. Das eHealth-Kartenterminal MUSS den sicheren PIN-Modus für die Abfrage von PINs gemäß den Erfordernissen des SICCT-Befehlssatzes aktivieren. Das Kartenterminal MUSS bei Eingabe einer Remote-PIN anzeigen, dass es sich um eine Remote-PIN-Eingabe (siehe [gemSpec_Kon#4.1.3.3.3]) handelt.

Die PIN DARF NICHT im Klartext am Kartenterminal dargestellt werden – insbesondere während der PIN-Eingabe. Es MUSS sichergestellt sein, dass die PIN nur maskiert (z. B. mittels Asterik ‚*') angezeigt wird und die Anzeige keine Rückschlüsse auf die PIN, abgesehen von deren Länge, zulässt.

3.6.6 Terminal Managementverfahren

Die Managementschnittstellen zur Administrierung des eHealth-Kartenterminals erlauben das Abfragen und Ändern der sicherheitskritischen Konfiguration erst nach erfolgreicher Authentisierung. Der Port des Administrationsservices DARF NICHT gleich dem SICCT Port sein. Die LAN Schnittstelle zur Administrierung MUSS mittels TLS gesichert sein. Als Authentisierungsverfahren für diese administrative TLS-Verbindung MUSS mindestens einseitige Authentisierung eingesetzt werden[8]. Zur Sicherung der administrativen TLS-Verbindung KANN auch gegenseitige Authentisierung eingesetzt werden. Im Fall der einseitigen Authentisierung MUSS sich das Kartenterminal (Server) gegenüber dem Client (z.B. Webbrowser) authentisieren. Falls eine SM-KT vorhanden ist, MUSS für den TLS Aufbau das Schlüsselmaterial der SM-KT verwendet werden (ID.SMKT.AUT). Falls keine SM-KT vorhanden ist, MUSS das Kartenterminal Schlüsselmaterial sowie ein zugehöriges Zertifikat zur Verfügung stellen (z. B. in der Firmware). Schlüsselmaterial, zugehöriges Zertifikat und verwendete Algorithmen MÜSSEN hierbei den Anforderungen gemäß [gemSpec_Krypt#5.1.1] entsprechen.

Dabei werden zwei Rollen unterschieden:

- Benutzer
- Administrator.

Der Benutzer ist nur berechtigt, die aktuellen Einstellungen anzuzeigen und sein eigenes Kennwort zu ändern. Für Kennwörter zur Sicherung der Managementschnittstelle gelten folgende Anforderungen. Kennwörter MÜSSEN mindestens 8 Zeichen lang sein und das Kennwort MUSS eine Mischung alphabetischer und nicht-alphabetischer Zeichen (Zahlen, Satzzeichen oder Sonderzeichen) oder eine Mischung von mindestens zwei Arten von nicht-alphabetischen Zeichen enthalten. Die Benutzer-ID DARF NICHT Bestandteil des Kennwortes sein. Das Kennwort MUSS spätestens nach 90 Tagen geändert werden, wobei beim Kennwortwechsel die letzten vier genutzten Kennworte NICHT als gültiges Kennwort akzeptiert werden DÜRFEN. Die Hashwerte der angegebenen Zahl von Kennwörtern MÜSSEN für mindesten 180 Tage gespeichert werden. Neue Kennwörter DÜRFEN NUR dann akzeptiert, werden wenn sie nicht mit den verwendeten gespeicherten Kennwörtern übereinstimmen. Wenn für das Passwort nur Ziffern zur Verfügung stehen, sollte es mindestens 6 Zeichen lang sein und das Authentisierungssystem sollte den Zugang nach wenigen Fehlversuchen sperren (für eine bestimmte Zeitspanne oder dauerhaft). Es ist auch der vom BSI herausgegebene Maßnahmenkatalog Organisation (M 2) Abschnitt 11 „Regelungen des Passwortgebrauchs“ [BSI-M2.11] zu beachten.

Das Einsehen der aktuellen Konfiguration MUSS geschützt werden, da die Daten der Terminalkonfiguration Informationen enthalten können, die für DoS und ähnliche Attacken benutzt werden können.

Der Administrator darf Einstellungen zur Benutzerverwaltung, Netzwerkkonfiguration, den Terminal- und Slot-Namen gemäß Abschnitt 4.11 ändern und Pairinginformation gemäß Abschnitt 3.7.2 löschen.

[8] Im Gegensatz zur SICCT-TLS-Verbindung, bei der nur gegenseitige Authentisierung erlaubt ist.

3.6.7 Spezielle SigG Anforderungen

Die Durchführung einer qualifizierten Signatur wird im Sinne des Signaturgesetzes (Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) vom 16.Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 1 des ersten Gesetzes zur Änderung des Signaturgesetzes [SigÄndG] vom 04.Januar 2005 (BGBl. I S. 2), geregelt.

Werden qualifizierte Signaturen durchgeführt, sind die Kartenterminals gemäß den konkretisierten Anforderungen der Signaturverordnung [SigV01] zu evaluieren und von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) oder einer akkreditierten Bestätigungsstelle zu bestätigen. Diese Bestätigung wird durch ein Prüfzeichen, welches von der gematik vergeben wird und auf dem Kartenterminal aufgebracht ist, angezeigt (siehe Kapitel 3.5.11).

3.6.8 Protection Profile

Protection Profiles für Kartenterminals legen die Mindestanforderungen im Sinne von Sicherheitszielen für ein Signaturterminal fest und beschreiben Funktionalitätsklassen. Protection Profiles dienen als Basis zur Durchführung einer Evaluierung des umfassenden Produkts.

Weitere Sicherheitsfunktionen von Kartenterminals, die über die Anforderungen an ein Signaturterminal hinausgehen, werden in die anschließende Evaluierung eingebunden oder erfordern zusätzliche Sicherheitsgutachten oder Evaluierungen.

3.6.8.1 Sicherheitsanforderungen LAN-gekoppelter Terminals

Die Sicherheitsanforderungen der eHealth-Kartenterminals orientieren sich entlang der Kommunikationskanäle und Funktionen:

- Anforderungen aus der Funktion im Rahmen der qualifizierten Signaturerstellung,
- sichere Identifikation und Authentisierung des Kartenterminals durch den Konnektor mit Hilfe kryptographischer Verfahren,
- Schutz der Vertraulichkeit, Authentizität und Integrität der übertragenen Daten,
- Schutz des Zugangs zu administrativen Einstellungen am Kartenterminal mit einem Passwortmechanismus oder höherer Sicherheit (z. B. 2-Faktor-Authentifizierung).

Für die Sicherung der Netzwerkkommunikation MUSS für alle Kartenterminals mindestens TLS 1.0 (Transport Layer Security) gemäß [RFC2246] und die TLS Extension gemäß [RFC3546] als einheitliches auf Zertifikaten basierendes Verfahren verwendet werden. Zusätzlich SOLL auch TLS 1.1 gemäß [RFC4346] unterstützt werden. Dies deckt — im Zusammenspiel mit der hinter dem Zertifikat stehenden PKI sowie dem Pairing des Kartenterminals mit dem Konnektor — auch die Forderung nach der sicheren Identifikation und Authentisierung des Kartenterminals durch den Konnektor ab. Der zum Zertifikat (C.SMKT.AUT) gehörigen geheimen Schlüssel (PrK.SMKT.AUT) ist in einem manipulationsgeschützten Speicher (SM-KT) verwahrt, der einen unbefugten Zugriff auf das Schlüsselmaterial verhindert.

3.6.8.2 Umgebungsanforderungen für Kartenterminals

Nach aktuellen Spezifikationen ergeben sich aus Sicherheitssicht Anforderungen an die Sicherheit des Terminals (siehe SP_PIN_USE_2 in [gemSiKo#AnhE]):

Die Ausgestaltung der Kartenterminals bzw. der Umgebung MUSS so gestaltet sein, dass von der gematik nicht zugelassene oder möglicherweise kompromittierte Komponenten vom Karteninhaber erkannt werden können. Es DARF NICHT möglich sein,

- die geheimen Daten, die im sicheren PIN-Eingabegerät gespeichert sind (Schlüssel und PINs), in Erfahrung zu bringen oder zu verändern, oder
- eine Abhörvorrichtung innerhalb des Gerätes einzurichten oder
- die Hard- oder Software des sicheren PIN-Eingabegerätes zu verändern.

Solche Angriffe MÜSSEN am Gerät physischen Schaden in der Art anrichten, dass er beim weiteren Betrieb, bzw. vor der Wiederinbetriebnahme des Gerätes mit hoher Wahrscheinlichkeit entdeckt wird. In der kontrollierten Einsatzumgebung (siehe Kapitel 3.6.8.2.1) ist das Brechen von Gehäusesiegeln ebenfalls als eine derartige physische Beschädigung des Gerätes zu betrachten.

Diese übergreifende Sicherheitsanforderung resultiert aus dem Schutzbedarf der nachfolgenden Sicherheitsobjekte:

- Signatur-PIN und Qualifizierte Signatur des Leistungserbringers
  Die Qualifizierte Signatur des Leistungserbringers stellt sehr hohe Anforderungen an die Sicherheit der Signaturkomponenten (siehe [gemSiKo#AnhE]).
- PIN des Versicherten für Autorisierung des Zugriffs auf freiwillige Anwendungen. Der Schutzbedarf dieser Daten ist sehr hoch, u. a. bezüglich der Vertraulichkeit, und äquivalent zu der PIN für die qualifizierte Signatur (siehe [gemSiKo#AnhF5.11]). Der Versicherte muss die PIN an einem Gerät eingeben, das nicht in seiner Verantwortung ist.
- Session-Key oder Objekt-Schlüssel
  Der Session-Key, der den sicheren Kanal zwischen Konnektor und KT definiert, ist im KT im Klartext verfügbar. Dies gilt ebenso für Objektschlüssel zur Verschlüsselung langlebiger medizinischer Objekte.

Die Maßnahmen zum Schutz von diesen Informationsobjekten mit hohem und sehr hohem Schutzbedarf (z. B. PINs, Schlüssel, medizinische Daten) drücken sich im PP des Kartenterminals in organisatorischen Anforderungen der Einsatzumgebungen und sicherheitstechnischen Maßnahmen des Kartenterminals aus. Generell DÜRFEN Daten aus der Telematikinfrastruktur (TI) NICHT persistent im Kartenterminal gespeichert werden, außer (und dieses ist die einzige Ausnahme) Konfigurationsdaten zwischen Konnektor und Kartenterminal (inkl. Shared Secret für das Pairing, siehe Kapitel 3.7). Folgende typische Einsatzumgebungen von Kartenterminals werden im Gesundheitswesen unterschieden:

- Kontrollierte Einsatzumgebung
- Nicht überwachte Einsatzumgebung

Für jede der beiden Einsatzumgebungen wird ein eigenes Schutzprofil definiert. Dies hat zur Folge, dass hinsichtlich ihres physischen Schutzes und der organisatorischen Verpflichtung

des Leistungserbringers zwei unterschiedliche Typen von eHealth-Kartenterminals zur Ausgestaltung kommen können.

3.6.8.2.1 Anforderungen an kontrollierte Einsatzumgebung

Bestehende zum Signaturgesetz konforme Kartenterminals kommen derzeit ohne hohen physikalischen Schutz aus, da Anforderungen an eine sichere Umgebung in die Verantwortung des Signaturkarteninhabers gestellt werden (lokaler Anschluss an den PC, Verbindungskabel im Sichtbereich etc.) Der Signaturkarteninhaber hat dafür Sorge zu tragen, dass in der Arbeitsumgebung, in der eine sichere elektronische Signatur erstellt wird, die geforderten Rahmenbedingungen der nach [SigG01] bestätigten Komponenten und Verfahren eingehalten werden. Dazu hat der Leistungserbringer (siehe [BÄK_POL]) sowohl alle technischen als auch organisatorischen Maßnahmen zu ergreifen, welche nur einen befugten Zugriff auf diese Arbeitsumgebung ermöglicht.

Es wird als Umgebungsanforderung der Kartenterminals angenommen,

- dass sich der Nutzer vor der Inbetriebnahme durch die Kontrolle der Unversehrtheit der Siegel überzeugt, dass keine sicherheitstechnischen Veränderungen am Kartenterminal bzw. an den Kabelanschlüssen vorgenommen wurden. Der Leistungserbringer MUSS sich daher, vor jeder Verwendung des Terminals von der Unversehrtheit des Siegels überzeugen, falls das Terminal seit der letzten Verwendung unbeaufsichtigt war. Ein manipuliertes Terminal wird durch Veränderungen am Gehäuse oder an Veränderungen an den Sicherheitssiegeln erkennbar (siehe [TR-03120#9]).

- dass dem Benutzer eine unbeobachtete Eingabe der Identifikationsdaten (PIN) gewährleistet wird.

- dass der Benutzer die PIN über den Nummernblock des Kartenterminals eingibt und während der PIN-Eingabe den Status des Kartenterminals dahingehend überprüfen kann, ob der Modus der sicheren PIN-Eingabe aktiv ist (s. Kap.3.6.5).

Durch organisatorische Maßnahmen MUSS der Leistungserbringer die Möglichkeiten für einen Angriff verringern und die Sicherheitsrisiken vermindern. Dies beinhaltet beispielsweise, dass

- der unbeaufsichtigte Zugriff von unbefugten Personen auf das Terminal unterbunden ist (z. B. weil der Arzt bzw. vertrauenswürdiges Personal immer im Zimmer ist) und der Raum ansonsten verschlossen ist;

- ein unbeaufsichtigter Zugriff auf das Terminal für unbefugte Personen nicht lange genug möglich ist, um einen Angriff auszuführen;

- die Mitnahme von notwendigem Werkzeug oder manipulierter Nachbauten eines Kartenterminals in die kontrollierte Einsatzumgebung nicht möglich ist;

- das Praxispersonal mit den Sicherheitsvorkehrungen, die zum Schutz des Terminals notwendig sind, vertraut gemacht und geschult wird.

Bei Einhaltung dieser organisatorischen Maßnahmen stellt die Versiegelung des Terminals einen hinreichenden physischen Schutz dar. Weiterführende Anforderungen an die kontrollierte Einsatzumgebung sind dem Protection Profile [BSI-PP-0032] zu entnehmen.

3.6.8.2.2 Anforderungen an nicht-überwachte Einsatzumgebung

Da in einer nicht-überwachten Einsatzumgebung eine Einschränkung eines Angriffs durch organisatorische Maßnahmen nicht möglich ist, MUSS ein Angriff an dem Kartenterminal einen physischen Schaden in der Art anrichten, dass das Kartenterminal nicht mehr funktionsfähig ist. Eine reine Versiegelung eines Terminalgehäuses kann in einer solchen Umgebung nicht als geeignet erachtet werden.

3.7 Festlegungen zu Kartenterminalidentität und Schlüsselmanagement

Die maximal zulässige Dauer des Pollingintervalls zur Detektierung der Entnahme der SM-KT ist in Abstimmung.

Ergänzend zum Abschnitt 8.6 der SICCT-Spezifikation werden die Mechanismen zur Erstellung, Einbringung und Sicherung der Kartenterminalidentität und der damit verbundenen geheimen Schlüssel beschrieben.

Die KT-Identität besteht aus der Kombination

- einer SMKT-Identität (ID.SMKT.AUT) bestehend aus einem Schlüsselpaar (PuK.SMKT.AUT, PrK.SMKT.AUT) mit zugehörigem X.509 Zertifikat (C.SMKT.AUT) welche in einem sichern Schlüsselspeicher/einem Sicherheitsmodul (im Folgenden als SM-KT bezeichnet) mit einer sicheren Verarbeitung für den privaten Schlüssel umgesetzt werden MUSS und

- einem nachfolgend ausgehandeltem gemeinsamen Geheimnis zwischen Kartenterminal und Konnektor (im Folgenden als Shared Secret oder Pairing-Key bezeichnet, siehe auch 3.7.2).

Die SMKT-Identität wird — unter anderem — zur Identifikation und Schlüsselaushandlung zwischen der Signaturanwendungskomponente (des Konnektors) und dem Kartenterminal genutzt[9].Die SMKT-Identität und der Pairing-Key DÜRFEN NICHT für sich alleine als Identität des Kartenterminals gewertet werden. Siehe auch [gemPKI_KT].

Ziel des SM-KT ist es, den privaten Schlüssel gegen ein Auslesen bzw. Vervielfachen zu sichern. Intention dieses Schutzmechanismus ist es nicht, die Integrität der Kartenterminalfirmware gegen Angriffe zu schützen. Das SM-KT ist auf einer Karte in ID-000 Form aufgebracht; entweder auf einer eigenständigen Karte oder als zusätzliche Identität einer SMC-A oder SMC-B (siehe auch [TR-03120]). Das SM-KT wird durch Stecken in einen entsprechenden ID-000 Slot, oder mittels Adapter in einen Slot anderen Formats in das Kartenterminal eingebracht. Der Gehäusezugang zum Steckplatz der Karte, welche das SM-KT enthält, KANN anschließend durch das Aufkleben eines Siegels gesichert werden (siehe Kapitel 4.1.3). Das SM-KT enthält keine Informationen zur Bauart des Kartenterminals.

Um zu verhindern, dass das SM-KT aus einem eHealth-Kartenterminal entfernt wird und in ein anderes Kartenterminal gesteckt wird, das vom Administrator nicht für den Betrieb mit dem Konnektor vorgesehen ist, wird dem Kartenterminal eine 16 Byte große Kennung übergeben, die vom Konnektor erzeugt wurde. Diese Kennung ist ein Shared Secret zwischen Konnektor und Kartenterminal. Das Verfahren wird als Pairing bezeichnet und in Kapitel

[9] In einer LAN-Umgebung wird die „alleinige Kontrolle“ schwer darstellbar und kann nur über entsprechend sichere Identitäten und authentifizierte Verbindungen zu Kartenterminals wiederhergestellt werden.

3.7.2 beschrieben. Das Shared Secret wird im Terminal gespeichert und vor Auslesen geschützt, wobei die genauen Schutzmechanismen von der Einsatzumgebung des Terminals abhängen (s. Kap. 3.6.8.2 sowie [BSI-PP-0032]). In jedem Fall DARF das Shared Secret NICHT auf dem SM-KT gespeichert werden. Eine Verschlüsselung des Shared Secrets ist nicht erforderlich. Ein fortgeführter Betrieb der SICCT-spezifischen TLS-Verbindung ohne vorhandenen Sicherheitsanker in Form der SM-KT DARF NICHT möglich sein. Bei Entnahme des SM-KT MUSS das Kartenterminal eventuell aktive TLS-Verbindungen, die die korrespondierende SMKT-Identität zum Betreiben des TLS-Kanals nutzen, aktiv beenden. Dies kann bei Entnahme des SM-KT durch folgende Maßnahmen erreicht werden:

- aktive Maßnahmen, wie direkte Erkennung der Kartenentnahme oder regelmäßigem Pollen der Karte mit anschließend gezieltem Kanalabbau bei fehlender Karte. Bei regelmäßigem Polling DARF das Pollingintervall NICHT mehr als 5 Sekunden betragen.

- passive Maßnahmen, bei denen die SM-KT nur in einem Zustand des Geräts gesteckt oder entfernt werden kann, während dem keine TLS-Verbindung zur Ausführung von SICCT- bzw. EHEALTH Kommandos möglich ist (z. B. Zugang zum SM-KT Kartenschacht nur nach Entfernen der LAN- und Powerkabel möglich)

Falls ein SM-KT entfernt wird, welches nicht die zum Verbindungsaufbau des TLS-Kanals verwendete SMKT-Identität enthält, ist es nicht erforderlich eventuell aktive TLS-Verbindungen aktiv zu beenden.

3.7.1 Anforderungen an die Kartentermianlidentität

Aufgabe der gematik ist (u. a.) die Sicherstellung der Interoperabilität und Kompatibilität technischer Komponenten für die Nutzung der Telematikinfrastruktur. Darüber hinaus hat die gematik sicherzustellen, dass nur zugelassene Komponenten in der Telematikinfrastruktur eingesetzt werden. Festlegungen zu den zu diesen Identitäten gehörenden Zertifikaten und der verwendeten PKI sind in [gemPKI_KT] beschrieben.

3.7.1.1 Ausführung

Die SMKT-Identitäten werden durch asymmetrische Schlüssel und X.509-Zertifikate umgesetzt. Genauere kryptographische Festlegungen werden in [gemSpec_Krypt] getroffen. Festlegungen zu den zu diesen Identitäten gehörenden Zertifikaten sind in [gemPKI_KT] beschrieben.

Grundsätzlich MÜSSEN die Schlüssel der SMKT-Identitäten in einem sicheren Schlüsselspeicher hinterlegt sein. Dieser Schlüsselspeicher wird SM-KT genannt. Die SM-KT MUSS dabei:

(1) den privaten Schlüssel sicher schützen, d. h., dass sie den privaten Schlüssel NICHT herausgeben DARF und dabei auch physikalischen Angriffen widerstehen MUSS (Tamper Resistance),

(2) für den privaten Schlüssel Entschlüsselung und Verschlüsselung/Signatur für die Authentifizierung unterstützen, wobei für die Benutzung des privaten Schlüssels keine Benutzerverifikation erforderlich ist,

(3) dem Kartenterminal einen Zufallszahlengenerator mit einer Entropie von mind. 80 Bit bieten ,

(4) den öffentlichen Schlüssel frei auslesen lassen.

Die SM-KT hat den Fingerprint des enthaltenen X.509 Zertifikats für die SMKT-Identitäten lesbar aufgedruckt oder der Fingerprint wird der SM-KT zuordenbar auf einer gesonderten Liste mitgeliefert.

Das Zertifikat der SMKT-Identität auf der SM-KT entstammt einer PKI, sodass andere Komponenten prüfen können, ob es von einer Certificate Authority (CA) ausgestellt wurde, die berechtigt ist Komponentenzertifikate für SM-KTs auszustellen. Es kann zudem überprüft werden, ob das Zertifikat die technische Rolle „Kartenterminal“ enthält. Es ist keine Aufnahme einer Online-Verbindung zu jener PKI erforderlich, die das Zertifikat herausgegeben.

Eine PIN-Freischaltung dieser Chipkarte DARF NICHT notwendig sein.

Genaue Festlegungen zur Filestruktur und den Zugriffsrechten der SM-KT werden in [HPC-P3] getroffen.

3.7.1.2 Bedeutung für das Kartenterminal

Das bedeutet für das Kartenterminal, dass es für seine Authentifikation bei der TLS-Verbindung zum Konnektor auf die SM-KT für die Erstellung des Authentifizierungstokens zurückgreifen MUSS. Die TLS-Verbindung auf der Kartenterminal-Seite terminiert aber nicht in der SM-KT, sondern im Terminal selbst.

3.7.1.3 Produktion und Auslieferung

Produktion, Auslieferung und Inbetriebnahme MÜSSEN aufeinander abgestimmt sein und sicherstellen, dass nur integere Kartenterminals eine gültige KT-Identitäten erhalten und beim Leistungserbringer zum Einsatz kommen.

Diese Prozesse werden in Begleitdokumenten spezifiziert.

3.7.2 Pairing zwischen Konnektor und eHealth-Kartenterminal

Das Pairing zwischen Konnektor und eHealth-Kartenterminal versetzt den Konnektor in die Lage, Kartenterminals als vom Administrator für den Betrieb mit dem Konnektor vorgesehen, zu erkennen. Das Pairing ermöglicht es einem Kartenterminal und einem Konnektor, sich nach dem TLS-Verbindungsaufbau gegenseitig zu authentifizieren. Da die kryptographische Identität des Kartenterminals auf der SM-KT gespeichert ist, diese aber aus einem Kartenterminal entfernt werden und in einem anderen Terminal gesteckt werden könnte, schafft das Pairing eine logische Verbindung von Kartenterminal und SM-KT.

Die Pairinginformation MUSS am Kartenterminal in so genannten Pairingblöcken verwaltet werden. Ein Pairingblock MUSS mindestens drei öffentlichen Schlüssel von Konnektorzertifikaten und einen Shared Secret aufnehmen können. Alle öffentlichen Schlüssel, die in demselben Pairingblock gespeichert sind, korrespondieren zu dem ebenfalls in diesem Pairingblock gespeicherten Shared Secret.

Das Kartenterminal MUSS sicherstellen, dass auf die Shared Secrets nur im Rahmen ihrer Bestimmung zugegriffen werden kann. Insbesondere DARF es NICHT möglich sein, die Shared Secrets über externe Schnittstellen zu lesen. Die genaue Ausprägung des auslesegeschützten Speicherns des Shared Secrets im Kartenterminal hängt von der Einsatzumge-

bung des Kartenterminals ab (s. Kap. 3.6.8.2). In jedem Fall DARF das Shared Secret NICHT auf der SM-KT im Terminal gespeichert werden.

Das Kartenterminal MUSS über eine Möglichkeit verfügen zum Zwecke der Administration ganze Pairingblöcke, oder gezielt einzelne öffentliche Schlüssel aus einem Pairingblock, zu löschen und das Kartenterminal MUSS sicherstellen, dass ein solches Löschen von Paringinformationen nur im ADMIN-Modus möglich ist. Das Kartenterminal MUSS mindestens einen Pairingblock speichern können. Das Kartenterminal SOLL mindestens zwei Pairingblöcke speichern können, um in einem mandantenfähigen Umfeld einsetzbar zu sein.

Gleichzeitige Verbindungen zu unterschiedlichen Konnektoren DÜRFEN NICHT möglich sein.

Das Pairing Konnektor/Kartenterminal MUSS sicher erfolgen. Der Administrator, der das Pairing der Kartenterminals durchführt, MUSS während des Prozesses sicherstellen, dass das Kartenterminal während des initialen Pairings (Schritt 1 und Schritt 2) in seiner organisatorischen Hoheit steht, so dass keine Dritten währenddessen Zugang zum Kartenterminal erlangen können. Im Rahmen des Pairings existieren vier Abläufe die im Folgenden beschrieben werden.

3.7.2.1 Initiales Pairing

Das initiale Pairing zwischen Konnektor und eHealth-Kartenterminal läuft in zwei Schritten ab:

1. Einbringen eines eHealth-Kartenterminals im Netzwerk des Leistungserbringers.
2. Inbetriebnahme eines eHealth-Kartenterminals an einem Konnektor.

Schritt 1: Einbringen eines eHealth-Kartenterminals im Netzwerk des Leistungserbringers:

Im ersten Schritt des Pairing-Verfahrens bringt der Administrator das eHealth-Kartenterminal ins LAN des Leistungserbringers ein. Der Administrator prüft die Unversehrtheit und Authentizität des eHealth-Kartenterminals, notiert sich dessen MAC-Adresse zusammen mit dem Fingerprint einer noch nicht zugeordnete SM-KT zur späteren Überprüfung und bringt diese SM-KT anschließend in das eHealth-Kartenterminal ein. Nachdem der Administrator ein oder mehrere eHealth-Kartenterminals derart im Netz des Leistungserbringers installiert hat, nimmt er jedes neu eingebrachte eHealth-Kartenterminal einzeln in Betrieb, damit der Konnektor und das eHealth-Kartenterminal sich gegenseitig als sicher erkennen und authentifizieren können.

Schritt 2: Inbetriebnahme eines eHealth-Kartenterminals an einem Konnektor.

Im zweiten Schritt, wählt der Administrator an der Kartenterminalverwaltung des Konnektors über die MAC-Adresse, die das Identifikationsmerkmal eines Kartenterminals in diesem Prozess bildet, ein eHealth-Kartenterminal aus, welches mit dem Konnektor gepairt werden soll.

Daraufhin baut der Konnektor eine TLS-Verbindung (siehe Kapitel 4.11) zum ausgewählten eHealth-Kartenterminal auf. Während dieses Verbindungsaufbaus erhält der Konnektor das X.509-Zertifikat der SM-KT (C.SMKT.AUT). Ist das Zertifikat ein gültiges SMKT-Komponentenzertifikat, zeigt der Konnektor dem Administrator den Fingerprint des SMKT-Komponentenzertifikats an, andernfalls bricht der Konnektor den Vorgang mit einer entsprechenden Fehlermeldung ab. Der Administrator überprüft, ob der vom Konnektor angezeigte Fingerprint mit dem in Schritt 1, für das zu pairende eHealth-Kartenterminal notierten SM-KT Fingerprint übereinstimmt. Stimmen beide Fingerprints überein, bestätigt der Administrator

dies dem Konnektor und startet dadurch den Austausch eines Shared Secrets zwischen Konnektor und eHealth-Kartenterminal.

Der Konnektor generiert eine 16-Byte große Zufallszahl (eHealth-Kartenterminal-Kennung bzw. auch als Shared Secret bezeichnet), und sendet die Kennung zusammen mit einer Displaymeldung[10] mit Hilfe des Pairingbefehls EHEALTH TERMINAL AUTHENTICATE über die TLS-Verbindung an das Kartenterminal. Das Kartenterminal MUSS die Displaymeldung anzeigen und MUSS auf eine Bestätigung mittels Druck auf die Bestätigungs-Taste am Pinpad warten. Wird die Bestätigungs-Taste nicht innerhalb einer herstellerspezifischen Zeitspanne, die maximal 10 Minuten betragen darf, gedrückt, oder wird der Abbruch-Button gedrückt, so MUSS das Kartenterminal den Vorgang mit einer entsprechenden Fehlermeldung abbrechen. Die Überprüfung des Kartenterminals vor Abschluss des Pairings durch den Administrator dient dazu, die Integrität und Authentizität des eHealth-Kartenterminals zum Zeitpunkt der Inbetriebnahme zu sicherzustellen.

Nachdem der Administrator mittels Tastendruck die Integrität und Authentizität des Kartenterminals bestätigt hat, speichert es den öffentlichen Schlüssel des Konnektorzertifikats in einem neuen Pairingblock. Schlägt die Prüfung fehl oder verfügt das Kartenterminal über keinen freien Pairingblock, bricht das Kartenterminal den Vorgang ab und zeigt eine entsprechende Fehlermeldung am Display.

Zum Abschluss des Prozesses sendet das Kartenterminal die mittels der SM-KT erstellte Signatur des Shared Secrets als Antwort des EHEALTH TERMINAL AUTHENTICATE Kommandos an den Konnektor. Der Konnektor prüft die Antwort. Kann er die Signatur erfolgreich prüfen, speichert der Konnektor das Shared Secret zusammen mit dem erhaltenen Kartenterminalzertifikat und der MAC-Adresse des Kartenterminals. Die Inbetriebnahme ist damit abgeschlossen.

3.7.2.2 Überprüfung der Pairinginformation durch einen Konnektor

Im Betrieb stellt der Konnektor über zwei Mechanismen sicher, dass ein eHealth-Kartenterminal ordnungsgemäß mit ihm gepairt wurde. Erstens, indem eine gegenseitige Authentisierung, zum Aufbau einer TLS-Verbindung erforderlich ist und zweitens, indem er die Pairinginformation in Form des Shared Secrets und des zugehörigen Zertifikats, welches beim TLS-Verbindungsaufbau verwendet wurde, prüft.

Diese Überprüfung eines eHealth-Kartenterminals durch einen Konnektor kann jederzeit nach dem TLS-Verbindungsaufbau zwischen Kartenterminal und Konnektor durch den Konnektor initiiert werden. Dafür schickt der Konnektor das EHEALTH-Kommando TERMINAL AUTHENTICATE (s. Kap. 4.7.2) an das Kartenterminal. Mit dem Kommando wird an das Terminal ein mindestens 16 Byte großes Zufallsdatum/-wert übertragen. Das Kartenterminal hängt an das Zufallsdatum das korrespondierende Shared Secret, aus den Pairinginformationen, und errechnet dann von dem kompletten Array den SHA-256-Hashwert. Diesen Hashwert schickt das Kartenterminal als Response zurück an den Konnektor.

Da der Konnektor ebenfalls das Shared Secret kennt, kann auch er den Hashwert errechnen. Das Kartenterminal hat nur dann die Überprüfung durch den Konnektor bestanden, wenn beide Hashwerte, der vom Kartenterminal geschickte und der vom Konnektor errechnete, identisch sind.

[10] Die Displaymeldung kann z. B. „Kartenterminal mit [MAC-Adresse] integer?“ lauten

3.7.2.3 Außerbetriebnahme

Zur Außerbetriebnahme eines eHealth-Kartenterminals MÜSSEN alle Pairinginformationen am Kartenterminal gelöscht werden.

3.7.2.4 Wartungspairing

Eine Ausnahme, die zum Austausch des Konnektors, z. B. zu Wartungszwecken, oder zur Umsetzung eines Hot-Standby vorgesehen ist, stellt das im Folgenden beschriebene Verfahren dar. Um zu verhindern, dass bei Ausfall eines Konnektors alle Kartenterminals erneut eingesammelt[11] und erneut dem initialen Pairing-Prozess zugeführt werden müssen, kann man eine Sicherungskopie der Pairing-Geheimnisse in den neuen Konnektor einspielen und mit deren Hilfe automatisiert ein neuerliches Pairing mit derselben Pairinginformation durchführen. Der Mechanismus zum Übertragen von Pairinginformationen zwischen zwei Konnektoren ist in [gemSpec_Kon#4.1.3.2.5] beschrieben.

Das Bekanntmachen eines neuen Konnektors unter Verwendung bereits bestehender Pairinginformation läuft in 2 Phasen ab. Nach dem TLS-Verbindungsaufbau ruft der Konnektor in der ersten Phase vom Kartenterminal mittels des EHEALTH TERMINAL AUTENTICATE mit P2=03 Kommandos eine Challenge (eine vom Kartenterminal generierte Zufallszahl) ab. Der Konnektor bildet aus der Challenge und dem Shared Secret den SHA256-Hashwert. Diesen Hashwert sendet der Konnektor in der zweiten Phase mittels des EHEALTH TERMINAL AUTENTICATE mit P2=04 Kommandos als Response auf die Challenge. Das Kartenterminal bildet für jeden genutzten Pairingbock ebenfalls den Hashwert aus Challenge und jeweiligem Shared Secret und vergleicht alle generierten Hashwerte mit der Response des Konnektors. Falls das Kartenterminal die Response erfolgreich validieren und eindeutig einem Pairingblock zuordnen kann, trägt das Kartenterminal den öffentlichen Schlüssel in den korrespondierenden Pairingblock ein. Falls kein Platz für einen weiteren öffentlichen Schlüssel im korrespondierenden Pairingblock vorhanden ist, überschreibt das Kartenterminal den ältesten öffentlichen Schlüssel des Pairingblocks.

Um eine logische Verbindung zwischen der Challenge und der Response am Kartenterminal herzustellen, nimmt das Kartenterminal im Kommando EHEALTH TERMINAL AUTHENTICATE mit P2=03 den Zustand „EHEALTH EXPECT CHALLENGE RESPONSE“ ein. Eine Response kann vom Kartenterminal nur in diesem Zustand validiert werden. Ist das Kartenterminal nicht in diesem Zustand wenn es eine Response auf eine Challenge erhält, schlägt der Befehl automatisch fehl. Sobald das Kartenterminal einen anderen Befehl als EHEALTH TERMINAL AUTHENTICATE mit P2=04 empfängt bzw. während der Validierung, verliert es den Zustand und löscht dabei auch die generierte Challenge.

[11] Im Gegensatz zum initialen Pairing muss der Administrator beim Wartungspairing nicht sicherstellen, dass sich alle Kartenterminals in seiner organisatorischen Hoheit befinden.

4 Spezielle technische Anforderungen (normativ)

Ein eHealth-Kartenterminal für den Einsatz im deutschen Gesundheitswesen kann aufgrund verschiedener Einsatzfälle unterschiedliche Bauformen haben. Insbesondere kann die Anzahl und Ausstattung von Kartensteckplätzen stark variieren.

Die Beschreibung der Kartenschnittstelle ist auf den Einsatz kontaktbehafteter Gesundheitskarten abgestimmt. Die Basis für alle Anforderungen ist die internationale Normenreihe ISO/IEC 7816.

In diesem Kapitel werden daher nur die Bezüge zur SICCT-Spezifikation angegeben und zudem besondere Einschränkungen oder auch zusätzliche Anforderungen beschrieben.

4.1 Abgeleitete mechanische Anforderungen

Die nachfolgenden Kapitel beschreiben mechanische und elektromechanische Anforderungen für die Teilgebiete Kartentypen, Kontaktiereinheiten und Bauformen.

4.1.1 Kartentypen

Der Heilberufsausweis (HBA), die Gesundheitskarte (eGK) und die Krankenversichertenkarte (KVK) verlangen kontaktbehaftete Schnittstellen mit Kartenkontaktiereinheiten der Größe ID-1 (mit den Maßen 85,6mm x 54,0mm) entsprechend der Norm ISO/IEC 7810 [ISO7810].

Die Security Module Card (SMC) ist eine kontaktbehaftete Karte im Format ID-1 oder ID-000 (Plug-in-Karte) nach CEN ENV 1375-1 [CEN ENV]. Die Spezifikation der eingesetzten Secure Module Cards erfolgt in [HPC-P3].

Die Lage und die Zuordnung der Kontakte ergibt sich aus ISO/IEC 7816-2 [ISO7816-2].

4.1.2 Kontaktiereinheiten

Generell sind alle Kontaktierungstypen zulässig, sofern die generellen mechanischen Anforderungen der folgenden Abschnitte eingehalten werden.

Allgemein gilt, dass im eHealth-Kartenterminal nur:

- kontaktschonende Kontaktiereinheiten verwendet werden dürfen,
- die Kartenkontakte C4, C6 und C8 nicht unterstützt werden,
- die Kartenkontakte C4, C6 und C8 elektrisch nicht angeschlossen werden.

Sind diese für spezielle Betriebsmodi wie ISO7816-12 erforderlich, so DÜRFEN diese NICHT vor Umschalten in einen solchen Modus aktiviert werden und MÜSSEN initial potentialfrei sein.

4.1.2.1 ID-1 Kartenkontaktierungen

Die Einführung oder Entnahme der Chipkarte DARF NICHT zu einer Beschädigung durch die Kontaktiereinheit führen.

Der „Card-In“-Schalter (d. h. der Schalter zur Kartenpräsenzerkennung) DARF NICHT vor Kontaktierung der Kontaktflächen und Erreichen des Kontakt-Enddrucks geschaltet werden. Der Anpressdruck der Kontakte auf die Kontaktflächen der Karte MUSS 0.2-0.6N betragen.

Der Chipkartenleser ist in der Lage, über ein Signal oder einen Status der Applikation zu melden, wann sich die Chipkarte korrekt in der Kontaktiereinheit befindet und wann diese mit Strom versorgt ist bzw. wenn diese entnommen wird.

In Ergänzung des Abschnitts 4.1.2 der SICCT-Spezifikation 1.20, ist bei Kartenlesern mit Entnahmeschutz auch sicherzustellen, dass eine gesteckte Karte auch nach einer Notentnahme noch funktionsfähig ist und keine mechanischen Beschädigungen durch die Entnahme aufweist. Das bedeutet, dass die Notentnahme ohne Risiken für die Karte (auch deren Bedruckung/Beschriftung) sein MUSS. Die Notentnahme SOLL nur durch das Bedienpersonal erfolgen können und sie MUSS vor Ort und mit gebräuchlichen Werkzeugen bzw. Hilfsmitteln durchführbar sein. Es MUSS aber nicht technisch sichergestellt sein, dass die Notentnahme nur durch das Bedienpersonal erfolgen kann, sondern, dies DARF mit Mechanismen im Rahmen der kontrollierten Einsatzumgebung des Leistungserbringers umgesetzt werden. Jedenfalls MUSS eine Bauform gewählt werden, die eine versehentliche Bedienung der Notentnahme verhindert[12]. Eine Notentnahme MUSS auch bei ausgefallener Stromversorgung möglich sein. Die notwendige Handhabung des Terminals für eine Notentnahme MUSS in der Benutzerdokumentation beschrieben sein.

Darüber hinaus werden Mechanismen empfohlen, um eine Notentnahme im Normalbetrieb eines Terminals zu unterbinden.

4.1.2.2 ID-000-Kartenkontaktierungen

Sofern native ID-000-Kontaktierungen vorhanden sind gilt:

- Der Zugriff auf die Plug-In-Karte(n) KANN möglich sein, eine Beschränkung des Zugangs zum Zwecke des Diebstahlschutzes ist nicht erforderlich.
- Es ist kein Card-In-Kontakt erforderlich.

4.1.3 Bauformen

Das eHealth-Kartenterminal, welches kontaktbehaftete Chipkarten unterstützt, besitzt mindestens eine Kontaktiereinheit zur Aufnahme von Chipkarten im Format ID-1.

Die Bauform mit einem einzelnen ID-1 Slot eignet sich jedoch nur, wenn entweder die eGK oder der HBA gesteckt wird. Es sind aber auch Anwendungen geplant, welche die gleichzeitige Anwesenheit von HBA und eGK erforderlich machen. Dazu sind zwei ID-1 Steckplätze empfohlen

Es MUSS mindestens zusätzlich eine Kontaktiereinheit vorhanden sein, sodass ein ID-000 Modul gesichert im Kartenterminal steckbar ist. Um etwaige Migrationsschritte unterstützen

[12] Es würde z. B. eine durch Drücken eines, im Gehäuse versenkten und nur durch z.B. eine Büroklammer erreichbaren, Knopfes ausgelöste Notentnahme diese Anforderung erfüllen.

zu können, SOLLEN mindestens zwei Kontaktiereinheiten zur sicheren Aufnahme von ID-000 Modulen verfügbar sein. Das Format der für die Aufnahmen von ID-000 Modulen bestimmten Kontaktiereinheiten ist herstellerspezifisch, da das ID-000 Modul auch mittels eines Adapters gesteckt werden KANN.

4.2 Abgeleitete elektrische Anforderungen

Details zu den Anforderungen sind der SICCT-Spezifikation zu entnehmen.

4.2.1 Elektrische Anforderungen für kontaktbehaftete Karten

Die Anforderungen in der SICCT-Spezifikation ergeben sich aus Teilaspekten der ISO/IEC 7816-3 [ISO7816-3] und der EMV 2004 [EMV_41]. Das eHealth-Kartenterminal bedient in erster Linie ISO/IEC kompatible Chipkarten und daher ist der ISO/IEC 7816-3 [ISO7816-3] Standard maßgeblich.

Zur Vermeidung von Ausfällen und Blockaden in der Applikation sind beim Einsatz vom EMV Terminals ISO Ergänzungen vorzunehmen, die möglicherweise eine Umschaltung gemäß SICCT-Spezifikation erforderlich machen. In einem solchen Fall ist der ISO-Betriebsmodus als Voreinstellung vorzusehen.

4.2.2 Reset-Verhalten und ATR-Bearbeitung

In Ergänzung zu den in Abschnitt 4.2.2 der SICCT-Spezifikation 1.20 [SICCT] genannten Anforderungen an das Kommunikationsverhalten des Kartenterminals, gelten die folgenden Mindestanforderungen für eHealth-Terminals:

- Parameter F_n 372 und 512
- Parameter D_n bei 372 1, 2, 4, 12
- Parameter D_n bei 512 1, 2, 4, 8, 16, 32

4.3 Transport von Zeichen

Die Kartenkommunikation und das Reset-Verhalten sind gemäß SICCT und ISO-7816-3 und -10 umzusetzen.

4.4 Chipkartenprotokolle

Das eHealth-Kartenterminal unterstützt nachfolgend aufgeführte synchrone und asynchrone Übertragungsprotokolle zu den entsprechenden Chipkarten. Die Protokolle sind nach den Vorgaben der jeweiligen internationalen Normen und der SICCT Spezifikation zu implementieren. Insbesondere MUSS allen Fehlerfällen wirksam begegnet werden und es DARF NICHT zum Auftreten einer Deadlock-Situation kommen.

Die Unterstützung von synchronen Karten Typ 1 (wie für die KVK genutzt) wird für die Migrationsphase gefordert. Nach Ende der Migration der Krankenversichertenkarte entfällt diese Anforderung automatisch.

Erforderliche Kartenprotokolle:

Asynchrone Chipkartenprotokolle

- T=1, Block-orientiertes Halbduplex-Protokoll gemäß ISO/IEC 7816-3 [ISO7816-3]

Synchrone Chipkartenprotokolle

Für synchrone Karten ist die Norm ISO/IEC7816-10 [ISO7816-10] einzuhalten.

- S=10 für 2-Wire-Bus Chipkarten gemäß ISO/IEC 7816-10 [ISO7816-10] und dort referenzierter Spezifikationen
- S=8 für I2C-Bus Chipkarten gemäß ISO/IEC 7816-10 [ISO7816-10]
- S=9 für 3-Wire-Bus Chipkarten nach Herstellerspezifikation und ISO/IEC 7816-10 [ISO7816-10]

Kontaktlose Chipkarten und Protokolle

Die Unterstützung von kontaktlosen Karten gemäß der SICCT-Spezifikation [SICCT], Abschnitt 4.3.2, ist nicht erforderlich. Sollten kontaktlose Karten unterstützt werden, so DARF deren Implementierung die Sicherheit des Gesamtsystems NICHT verletzen.

4.5 Isolation von Verbindungen zum Kartenterminal

eHealth-Kartenterminals MÜSSEN den Kontext der von ihnen verwalteten Chipkarten lokal zur jeweiligen Verbindung eines Hosts halten. Dies bedeutet, dass mit einem Verbindungsabbruch für alle Karten des Terminals, die sich in Verwendung des davon betroffenen Hosts befinden, ein Reset der Karten erfolgen MUSS.

4.6 Gleichzeitige Verbindungen zum Kartenterminal

eHealth-Kartenterminals dürfen abweichend von und ergänzend zu den Vorgaben der SICCT Spezifikation auch mehrere Verbindungen zu ansteuernden Hosts unterhalten. Hosts können hierbei ein Konnektor und Konfigurationsprogramme der Terminal-Hersteller sein. Es DARF NICHT möglich sein, gleichzeitig Verbindungen zu mehr als einem Konnektor zu unterhalten. Es DARF NICHT möglich sein mehrere Verbindungen über den SICCT-Port zu unterhalten. Für jede Verbindung gilt, dass diese als eigener Kontext verwaltet werden MUSS und Ressourcen NICHT gleichzeitig genutzt werden DÜRFEN. Ein Übergang des Nutzungsrechts für Ressourcen zwischen diesen Kontexten ist nur in einem sicheren Zustand der jeweiligen Ressourcen (z. B. unmittelbar nach dem Reset einer Chipkarte) gestattet.

Grundsätzlich gelten die Bestimmungen für die gleichläufige Abarbeitung gemäß SICCT-Spezifikation [SICCT], Abschnitt 5.5.4 und 6.1.4.3.

Wenn über die lokale Schnittstelle eine Verbindung zum Kartenterminal aufgebaut ist, MUSS die Verbindung über LAN zum Konnektor abgelehnt, beziehungsweise eine bestehende Verbindung abgebrochen sowie die Karten zurückgesetzt werden. Dies ist notwendig, um für LAN-Verbindungen zum Konnektor den vertrauenswürdigen Modus zu erhalten, da der lokale Anschluss als unsicher angesehen wird. Es ist nicht bekannt wer über den lokalen Anschluss zugreift.

4.7 Kartenterminalkommandos

Alle eHealth-Kartenterminals MÜSSEN aus Gründen der Interoperabilität über den gleichen Kommandosatz zur Ansteuerung verfügen.

Die Kommandos des SICCT-Betriebsmodus gemäß Abschnitt 5.5.7 der SICCT-Spezifikation [SICCT] sind verpflichtend vollumfänglich zumindest für die (Ethernet-)Netzwerk-Schnittstellen des Kartenterminals zu implementieren.

Die Kommandos des BCS-Betriebsmodus gemäß Abschnitt 5.5.6 der SICCT-Spezifikation [SICCT] sind zumindest für die V.24-Schnittstelle des Kartenterminals verpflichtend zu implementieren, sofern ein Kartenterminal über optionale V.24-Schnittstellen verfügt. Wird ein Kartenterminal lokal von einem Konnektor z. B. über eine USB-, IEEE1284- oder FireWire-Schnittstelle angesteuert, so MÜSSEN hier die BCS-Kommandos über diese Protokolle getunnelt werden. Da es sich bei BCS um eine unverschlüsselte Kommunikation handelt, wird bei einer „lokalen Verbindung zu einem Konnektor“ von einer räumlichen Nähe von Kartenterminal und Konnektor ausgegangen.

Das Kartenterminal MUSS über einen mindestens 3 Kilobyte (KB) (3072 Byte) großen Kommandopuffer für APDUs verfügen. In diesen 3 KB ist der 10 Byte große SICCT-Envelope nicht enthalten.

Details sind der SICCT-Spezifikation [SICCT] Kapitel 5 zu entnehmen. Es gelten die nachstehenden Abänderungen und Ergänzungen.

4.7.1 Verbindlichkeit des SICCT-Kommandos CONTROL COMMAND

Abweichend von Kapitel 5.9 der SICCT-Spezifikation KANN das „CONTROL COMMAND“-Kommando entfallen und immer 6200 oder 64xx zurück gemeldet werden[13]. Ist das „CONTROL COMMAND“ Kommando jedoch vollständig implementiert, so MUSS sichergestellt werden, dass Kommandos des Konnektors nicht von Drittsystemen[14] abgebrochen werden können.

4.7.2 Command EHEALTH TERMINAL AUTHENTICATE

Das Kommando EHEALTH TERMINAL AUTHENTICATE dient dem Pairing von Konnektor und Kartenterminal. Mit Hilfe dieses Kommandos

[13] Ein e-Health-Konnektor (oder ein anderes Client-System) darf nicht voraussetzen, dass an ein Terminal übermittelte Kommandos abgebrochen werden können. Da der Erfolg oder Misserfolgs eines Abbruchs rein vom Zeitpunkt des Empfangs und der Verarbeitung des Abbruch-Kommandos abhängig ist, kann auch ein konsistenter Wegfall der Funktionalität akzeptiert werden.
[14] Drittsysteme sind alle Systeme, die nicht die Kommandoausführung veranlasst haben.

1) übergibt der Konnektor dem Kartenterminal das Shared Secret im Zuge des Pairing-Verfahrens.

2) prüft der Konnektor, ob das Kartenterminal das mit dem Konnektor ausgehandelte Shared Secret kennt, das zu der in dem Kartenterminal steckenden SM-KT gehört.

3) kann ein Konnektor der bereits über ein am Kartenterminal eingetragenes Pairinggeheimnis verfügt, sein Konnektor-Zertifikat am Kartenterminal bekannt machen und sich dadurch mit dem KT Pairen.

4.7.2.1 Funktion

Das Kommando hat drei Ausprägungen:

1. CREATE (P2='01'): Das Pairing des Kartenterminals erfolgt zu einem neuen Konnektor. Dies ist der Vorgang, der ausgeführt wird, wenn der betroffene Konnektor nicht über ein am KT hinterlegtes Shared Secret verfügt (z. B. beim initialen Pairing oder falls die Pairinginformation am Konnektor verloren gegangen ist).

2. VALIDATE (P2='02'): Der Konnektor prüft mittels Shared Secret, ob das Pairing zu dem Kartenterminal ordnungsgemäß erfolgt ist.

3. ADD (Schritt1: P2='03', dann Schritt2 P2='04'): Das Pairing des Kartenterminals erfolgt zu einem neuen Konnektor. Im Gegensatz zu CREATE ist dies der Vorgang, der ausgeführt wird, wenn der betroffene Konnektor bereits über ein am KT hinterlegtes Shared Secret verfügt (z. B. bei Austausch desjenigen Konnektors, bei dem eine Sicherungskopie der Pairinggeheimnisse verfügbar ist). Damit der Konnektor nachweisen kann, dass er über das korrekte Shared Secret verfügt, wird ein Challenge-Response Verfahren verwendet. Hierzu wird der Befehl in zwei Phasen aufgeteilt. In der ersten Phase (P='03') erbittet der Konnektor eine Challenge vom Kartenterminal und in der zweiten Phase (P='04') antwortet der Konnektor mit der Response. Wird die Antwort vom Kartenterminal erfolgreich validiert, nimmt das Kartenterminal den Konnektor als bekannten Konnektor auf. Diese Kommandoausprägung erlaubt ein automatisiertes Pairing und ist zu Wartungszwecken vorgesehen.

Details zu den Kommandoausprägungen sind der folgenden Kommandobeschreibung zu entnehmen.

Wird das Kommando mit P2='01' (CREATE) ausgeführt, läuft die Verarbeitung des Kommandos im Kartenterminal in (8) Schritten ab.

(1) Das Kartenterminal prüft, ob noch ein freier Pairingblock vorhanden ist. Ist dies nicht der Fall so bricht das Kartenterminal den Befehl mit einer entsprechenden Fehlermeldung ab (SW1SW2=6900).

(2) Das Kartenterminal prüft, ob der im Shared Secret DO übergebene Byte String genau 16 Byte lang ist. (Shared Secret). Ist dies nicht der Fall bricht das Kartenterminal mit Fehler ab (SW1SW2=6A80). Das Shared Secret ist eine vom Konnektor generierte Zufallszahl.

(3) Das Kartenterminal MUSS sicherstellen, dass die gespeicherten Shared Secrets und die gespeicherten öffentlichen Schlüssel für Konnektoren eindeutig sind. Hat es bereits ein identisches Shared Secret gespeichert, bricht das Kartenterminal mit Fehler ab (SW1SW2=6402). Hat das Kartenterminal den öffentlichen Schlüssel des beim Verbindungsaufbau präsentierten Konnektorzertifikats bereits gespeichert, MUSS es

diesen aus dem korrespondierenden Pairingblock löschen. Der Pairingblock bleibt jedenfalls erhalten, selbst wenn keine öffentlichen Schlüssel in ihm gespeichert sind.

(4) Das Kartenterminal prüft, ob ein Displaytext enthalten ist. Fehlt der Displaytext so bricht das Kommando mit Fehler ab (SW1SW2=6A80).

(5) Das Terminal zeigt den Displaytext an und wartet darauf, dass auf dem Pinpad die Bestätigungs-Taste gedrückt wird. Durch Druck der Abbrechen-Taste wird der Befehl abgebrochen. Wird nicht binnen einer herstellerspezifischen Zeitspanne die maximal 10 Minuten betragen darf, die Bestätigungs-Taste gedrückt, MUSS der Befehl abgebrochen werden. Bei Abbruch löscht das Kartenterminal das Shared Secret wieder aus seinem Speicher und schickt eine Fehlermeldung zurück. Bei Abbruch durch Tastendruck MUSS mit Fehlercode SW1SW2=6401 geantwortet werden. Bei Abbruch durch Timeout MUSS mit Fehlercode SW1SW2=6400 geantwortet werden.

(6) Das Kartenterminal speichert den im Shared Secret DO übergebenen Byte-String zusammen mit dem während des TLS-Aufbaus erhaltenen öffentlichen Schlüssel des Konnektorzertifikats in einem unbenutzten Pairingblock ab.

(7) Für das erhaltene Shared Secret wird mittels der SM-KT unter Verwendung des Zertifikats für die SMKT-Identität eine Signatur erstellt. Hierfür generiert das Kartenterminal den SHA-256-Hashwert des Shared Secrets. Dieser Hashwert wird durch die SM-KT mittels EMSA-PSS gemäß [PKCS#1] Kapitel 9.1 mit einer Moduluslänge von 2048 Bit signiert. Diese Verfahren stehen auf der SM-KT zur Verfügung.

(8) Die in Schritt (7) berechnete Signatur wird in der Response APDU zurückgeschickt.

Falls das Kommando mit P2=’02’ (VALIDATE) ausgeführt wird so läuft die Verarbeitung des Kommandos im Kartenterminal in 4 Schritten ab:

(1) Das Kartenterminal prüft, ob der im Shared Secret Challenge DO übergebene Byte-String mindestens 16 Byte lang ist. Ist dies nicht der Fall bricht das Kartenterminal mit Fehler ab (SW1SW2=6A80).

(2) Das Kartenterminal sucht anhand des öffentlichen Schlüssels des Konnektorzertifikats den Pairingblock, der das korrespondierende Shared Secret enthält. Hierfür ist ein byte-weiser Vergleich der Schlüssel ausreichend. Hat das Kartenterminal den öffentlichen Schlüssel noch nicht gespeichert, bricht es mit einer Fehlermeldung ab (SW1SW2=6900).

(3) Hat das Kartenterminal in Schritt (2) ein korrespodierendes Shared Secret gefunden, hängt es an die Shared Secret Challenge das korrespondierende Shared Secret an.

(4) Von diesem in Schritt (3) generierten Array wird dann der SHA-256-Hashwert berechnet.

Der berechnete Hashwert wird in der Response-APDU an den Konnektor zurückgeschickt.

Falls eine Displaymessage angegeben wurde, wird diese ignoriert.

Falls das Kommando mit P2=’03’ oder P2=’04’ (ADD) ausgeführt wird so läuft die Verarbeitung des Kommandos im Kartenterminal in 2 Phasen ab. Für P2=’03’ (ADD Phase 1) ist der Ablauf wie folgt:

(1) Das Kartenterminal erzeugt mittels des Zufallszahlengenerators der SM-KT eine mindestens 16-Byte lange Zufallszahl.

(2) Das Kartenterminal geht in den Zustand „EHEALTH STATE EXPECT CHALLENGE RESPONSE“ über und speichert die Zufallszahl auslesegeschützt ab.

(3) Das Kartenterminal sendet die in (1) generierte Zufallszahl in der Response-APDU an den Konnektor zurück.

Für P2=’04’ (ADD Phase 2) ist der Ablauf wie folgt:

(1) Das Kartenterminal prüft ob es sich im Zustand „EHEALTH STATE EXPECT CHALLENGE RESPONSE“ befindet. Ist dies nicht der Fall bricht das Kartenterminal mit einem Fehler ab (SW1SW2=6900).

(2) Das Kartenterminal verlässt den Zustand „EHEALTH STATE EXPECT CHALLENGE RESPONSE“

(3) Für jeden genutzten Pairingblock berechnet das Kartenterminal aus der in Phase 1 generierten Zufallszahl und dem Shared Secret des jeweiligen Pairingblocks die SHA-256 Hashwerte (vgl. Ablauf bei P2=’02’) und löscht anschießend die generierte Zufallszahl.

(4) Das Kartenterminal vergleicht alle generieren Hashwerte mit der im Shared Secret Response DO enthaltenen Antwort des Konnektors.

(5) Stimmt genau einer der Hashwerte überein, selektiert das Kartenterminal den Pairingblock, der das erfolgreich geprüfte Shared Secret enthält, um dort den öffentlichen Schlüssel des beim TLS-Verbindungsaufbaus erhaltenen Konnektorzertifikats einzutragen. Sonst bricht das Kartenterminal mit Fehler ab (SW1SW2=6400). Die Regeln für das Eintragen des neuen öffentlichen Schlüssels sind dabei wie folgt:

a) Ist der öffentliche Schlüssel bereits im selektierten Pairingblock enthalten, trägt das Kartenterminal den Schlüssel nicht ein und antwortet mit einem Command successful (SW1SW2=9000).

b) Ist der neue öffentliche Schlüssel noch nicht im selektierten Pairingblock enthalten und ist noch mindestens ein Speicherslot für öffentliche Schlüssel im Pairingblock frei, wird der neue öffentliche Schlüssel hinzugefügt und das Kartenterminal antwortet mit einem Command successful (SW1SW2=9000).

c) Ist der neue öffentliche Schlüssel noch nicht im selektierten Pairingblock enthalten und ist kein Speicherslot für öffentliche Schlüssel im Pairingblock mehr frei, wird der älteste öffentliche Schlüssel, jener dessen Pairingvorgang am längsten zurück liegt, mit dem neuen öffentlichen Schlüssel überschrieben und das Kartenterminal antwortet mit einem Command successful (SW1SW2=9000).

4.7.2.2 Der Zustand EHEALTH EXPECT CHALLENGE RESPONSE

Dieser Zustand dient dazu einen unmittelbaren Zusammenhang zwischen dem Kommando EHEALTH TERMINAL AUTHENTICATE mit (P2=’03’) und EHEALTH TERMINAL AUTHENTICATE mit (P2=’04’) herzustellen.

Das Kartenterminal MUSS diesen Zustand verlieren und die in EHEALTH TERMINAL AUTHENTICATE mit (P2=’03’) generierte Challenge löschen, sobald ein anderes Kommando als das EHEALTH TERMINAL AUTHENTICATE mit (P2=’04’) ausgeführt wird. Das Kartenterminal MUSS sicherstellen, dass es diesen Zustand nur durch den Befehl EHEALTH

TERMINAL AUTHENTICATE mit (P2='03') einnehmen kann. Das Kartenterminal MUSS den Zustand nach maximal 30 Sekunden verlieren und dabei auch die generierte Challenge löschen.

4.7.2.3 Anwendungsbedingungen

Das Kartenterminal MUSS sich im SICCT Modus befinden, um das Kommando auszuführen.

4.7.2.4 Command Structure

EHEALTH Kommando	Kodierung C-APDU						
	CLA	INS	P1	P2	[Lc]	[Data]	[Le]
EHEALTH TERMINAL AUTHENTICATE	'81'	'AA'	Functional Unit	Command Qualifier	Length Command Data	Command Data	Length Requested Data
	§ CLA = Class § INS = Instruction § P1, P2 = Parameter 1 and 2 § Lc = Length of command data field § Le = Length of expected § SW1, SW2 = Status Bytes				Case 2 (no cmd data, rsp data:) no Lc Le=1-255 Bytes Case 3 (cmd data, no rsp data:) Lc=1-255 Bytes no Le Case 4 (cmd data, rsp data): Lc=1-255 Bytes Le=1-256 Bytes		

Specification C-APDU		
CLA	'81'	Cardterminal Command Class
INS	'AA'	EHEALTH TERMINAL AUTHENTICATE

P1	Functional Unit		
	bit8 .. bit1	Direct Coding (mandatory)	
		'00'	Address Cardterminal

P2	Command Qualifier		
	bit8..bit1	'01'	create Pairingblock for new Shared Secret and Konnektor
		'02'	authenticate with Shared Secret
		'03'	generate Challenge
		'04'	add Konnektor to known Pairingblock
		other values RFU	

Lc	Length of Command Data Nc	
	Direct coding	
	P2=01	Lc short; ’12’<=Lc<=’FF’
	P2=02	Lc short; ’12’ <= Lc <=’81’
	P2=03	absent
	P2=04	Lc short Lc=’22’

Data	Command Data		
	In Case of P2=01		
	Shared Secret DO	Byte sequence: Shared secret generated by Kon-nektor during pairing	see Chapter 0
	APPLICATION LABEL DO	Text / display Message	see SICCT 5.5.10.19
	SICCT Message To Be displayed DO	Constructed TLV-DO con-taining one character set and one Application Label DO	see SICCT 5.5.10.21
	In Case of P2=02		
	Shared Secret Challenge DO	Byte sequence: Random Bytes	see Chapter 4.7.2.8
	In Case of P2=03: absent		
	In Case of P2=04		
	Shared Secret Response DO	SHA-256 Hashvalue	see Chapter 4.7.2.9

Le	Length of Requested Data Ne Return up to Ne bytes of requested information		
	In case of P2=01		
	bit8..bit1	’00’	Expect ‘100’ byte long signature (2048 bit mode)
	In case of P2=02		
	bit8..bit1	‘20’	Expect ‘20’ byte long hashvalue
	In Case of P2=03		
	bit8..bit1	‘10’..’7F’	Expect ‘10’ to ‘7F’ byte long Challenge
	In Case of P2=’04’: absent		

4.7.2.5 Response Structure

EHEALTH TERMINAL AUTHENTICATE	Kodierung R-APDU			
	[Body:]		**Trailer**	
	[Requested Data / Information]		Status Byte 1	Status Byte 2
	Requested data	in case of success and P2=01 : Signature of Shared Secret created with Certificate of SM-KT	SW1	SW2

	Requested data	in case of success and P2=02: SHA-256 hash value		
	Empty	in case of error		

4.7.2.6 Status-Codes SW1-SW2

Nachstehend sind die Kommando-spezifischen Fehler beschrieben. Allgemeine Fehler gemäß SICCT-Spezifikation sind nicht gesondert berücksichtigt.

SW1SW2	P2	Specification	Meaning
6400	'01' CREATE	Execution Error	Nor or incomplete input in time
	'03' ADD	Execution Error	Hashvalue not found
6401	'01' CREATE	Execution Error	Process aborted by pressing of CANCEL key
6402	'01' CREATE	Execution Error	Duplicate Shared Secret
6900	'01' CREATE	Command not allowed	No unused pairing block available
	'02' VALIDATE	Command not allowed	Presented Public Key unknown
	'03' ADD	Command not allowed	CT is not in the state "EHEALTH EXPECT CHALLENGE RESPONSE"
6A80	'01' CREATE	Incorrect Parameters	Length of SS DO is not 16 bytes or No Displaymessage given.
	'02' VALIDATE	Incorrect Parameters	Length of SS DO is smaller than 16 bytes

4.7.2.7 Shared Secret Data Object

Das Shared Secret Data Object enthält das vom Konnektor während des Pairingvorgangs generierte Shared Secret.

Shared Secret Data Object (SS DO)			
TAG	'D4'	One byte tag according ISO 7816-6: Application Label	
		Tag coding according ASN.1 BER see SICCT 5.5.10.3	
		BER-Coding : private, primitive, Tag-Number = 20 ('14')	
Issue LEN	LEN coding see SICCT 5.5.10.3		
	'10'	one byte coding LEN = 16	
	all other values	reject with error	
VALUE	Shared Secret		
	Byte Sequence containing Shared Secret		

4.7.2.8 Shared Secret Challenge Data Object

Das Shared Secret Challenge Data Object enthält die vom Konnektor zur Überprüfung der Pairinginformation des Kartenterminals gesendete Challenge.

Shared Secret Challenge Data Object (SSC DO)			
TAG	'D5'	One byte tag according ISO 7816-6: Application Label	
		Tag coding according ASN.1 BER see SICCT 5.5.10.3	
		BER-Coding : private, primitive, Tag-Number = 21 ('15')	
LEN	LEN coding see SICCT 5.5.10.3		
	'10'..'7F'	one byte coding 16 <= LEN <=127	
	'0'..'0F'	reject with error	
VALUE	Shared Secret Challenge		
	Random Byte Sequence		

4.7.2.9 Shared Secret Response Data Object

Das Shared Secret Response Data Object enthält die vom Konnektor zur Überprüfung der Pairinginformation des Konnektors gesendete Response.

Shared Secret Response Data Object (SSR DO)			
TAG	'D6'	One byte tag according ISO 7816-6: Application Label	
		Tag coding according ASN.1 BER see SICCT 5.5.10.3	
		BER-Coding : private, primitive, Tag-Number = 22 ('16')	
LEN	LEN coding see SICCT 5.5.10.3		
	'10'	one byte coding LEN=16	
	all other values	reject with error	
VALUE	Shared Secret Response		
	Random Byte Sequence		

4.7.3 Ergänzung des Command SICCT OUTPUT

Das Kartenterminal MUSS die mittels SICCT OUTPUT übergebe Display-Nachricht gemäß [SICCT#5.6.1] zur Anzeige bringen können. Hierbei MUSS mindestens die Länge von 48 Zeichen einer Display-Nachricht unterstütz werden.

4.7.4 Ergänzung des Command SICCT PERFORM VERIFICATION

Das Kartenterminal MUSS die mittels SICCT PERFORM VERIFICATION übergebenen Parameter Display-Nachricht und Pinprompt gemäß [SICCT#5.6.1] zur Anzeige bringen können. Hierbei MUSS, abweichend von der SICCT Spezifikation, mindestens die Länge von 48 Zeichen für die Display-Nachricht unterstützt werden. Für das Pinpromt MUSS mindestens die Länge von 10 Zeichen unterstützt werden.

4.7.5 Ergänzung des CardTerminal Manufacturer Data Objects

Ergänzend zu Kapitel 5.5.10.6 der SICCT Spezifikation MUSS das CardTerminal Manufacturer Data Object CTM DO verpflichtend über das Discretionary Data Data Object (DD DO) verfügen. Das DD DO MUSS wie folgt aufgebaut sein:

<table>
<tr><td colspan="5">Discretionary Data Data Object (DD DO)</td></tr>
<tr><td rowspan="3">TAG</td><td rowspan="3">'D7'</td><td colspan="3">One byte tag according ISO 7816-6: Application Label</td></tr>
<tr><td colspan="3">Tag coding according ASN.1 BER see SICCT 5.5.10.3</td></tr>
<tr><td colspan="3">BER-Coding : private, primitive, Tag-Number = 23 ('16')</td></tr>
<tr><td rowspan="2">LEN</td><td colspan="4">LEN coding see SICCT 5.5.10.3</td></tr>
<tr><td colspan="4">52<=LEN<=110</td></tr>
<tr><td rowspan="5">VALUE</td><td>DO name</td><td></td><td>length</td><td>Description</td></tr>
<tr><td>ZLS</td><td>man</td><td>22</td><td>”Zulassungss-chlüssel” of Card-terminal</td></tr>
<tr><td>SER</td><td>man</td><td>15</td><td>Serial Number of Cardterminal</td></tr>
<tr><td>MODN</td><td>man</td><td>15</td><td>Model Name of Cardterminal</td></tr>
<tr><td>VEN</td><td>opt</td><td>0..58</td><td>Verdor specific in-formation</td></tr>
</table>

Data	Len		Description
ZLS	22	man	22 Byte ASCII String: of form ZLS_eHealth_[HST]_[nnnnnn] Values in brackets are determined as follows: • HST is the abbreviation of the Vendor. (3 Bytes)

			• nnnnnn is a consecutive vendor-specific number including one check digit (6 Bytes) Both, HST and nnnnnn are issued by the gematik
SER	15	man	15 Byte ASCII String- padded with Space ('20'). Vendor specific serialnumber of the Cardterminal
MODN	15	man	15 Byte ASCII String- padded with Space ('20') Vendor specific modelname of the Cardterminal
VEN	0..58	opt.	optional, vendor specific coded string.

Der Zulassungsschlüssel (ZLS), der für einen konkreten Firmware-Stand verwendet werden muss, wird dem Hersteller von der gematik bei der Anmeldung zur Zulassung bekanntgegeben.

4.8 Verhalten bei der PIN-Eingabe

Unabhängig davon, ob es sich um eine Eingabe von einer PIN mit variabler oder fixer Länge handelt, MUSS die Eingabe der PIN durch Drücken einer „Enter“-Taste (dies legt nicht die Beschriftung dieser Taste, sondern lediglich ihre Funktion bei der PIN-Eingabe fest) bestätigt werden. Dieses ergänzt die Funktionsbeschreibung von Abschnitt 5.19 der SICCT-Spezifikation [SICCT], wie auch andere Spezifikationsabschnitte, die eine PIN-Eingabe erfordern.

In Fällen, bei denen die zu erwartende, minimale PIN-Länge (entweder von einer Applikation übergeben oder durch das PIN-Format vorgegeben) unterschritten wird, ist die „Enter“-Taste keine gültige Eingabe und wird deshalb nicht akzeptiert[15].

Diese Anforderungen an die PIN-Eingabe entspringen sowohl den Benutzbarkeits- als auch den Sicherheitsanforderungen.

4.9 Festlegungen zur Sicherung der Firmware-Updates

Die Aktualisierung der Kartenterminal-Firmware MUSS mittels asymmetrischer kryptographischer Verfahren geschützt werden. Konkret wird nur eine Sicherung der Authentizität und Integrität gewährleistet werden. Dies ist durch eine Signatur durch den Terminalhersteller[16] zu gewährleisten. Das Format der Firmware (d. h. des Binärfiles) bleibt herstellerspezifisch.

[15] Dieses Verhalten entspricht dem von Geldautomaten.
[16] Die Signatur durch den Kartenterminal-Hersteller dient dazu sicherzustellen, dass bei der Übermittlung und den anschließenden Prüf- und Verarbeitungsschritten innerhalb der prüfenden und zulassenden Stelle keine beabsichtigten oder unbeabsichtigten Verfälschungen der Firmware („Bitdreher“) auftreten können.

Die Prüfung der einzuspielenden Firmwareversion erfolgt stets durch die zu diesem Zeitpunkt aktive Firmware, die auch die öffentlichen Schlüssel für die Signaturprüfung[17] enthalten MUSS.

4.10 Auswahl kryptographischer Algorithmen für TLS

Für die Transportverschlüsselung mittels TLS gemäß [SICCT, Abschnitt 6.3.1.1] ist die Unterstützung der in [gemSpec_Krypt#6.4.4] angegebenen Cipher Suites verpflichtend.

4.11 Authentisierung beim Aufbau der SICCT-spezifischen TLS-Verbindungen

Für den Aufbau der nach [SICCT#6.3.1.1] spezifizierten SICCT-spezifischen TLS-Verbindung, die zur Nutzung für eine Kommunikation gemäß SICCT-Protokoll vorgesehen ist, MUSS gegenseitige Authentisierung zwischen Server (Kartenterminal) und Client (Konnektor) umgesetzt werden. Andere Authentisierungsverfahren (einseitige Authentifizierung, Whitelist, …) zum Aufbau der SICCT-spezifischen TLS-Verbindung DÜRFEN NICHT eingesetzt werden. Diese Anforderungen gelten nicht für den Aufbau administrativer TLS-Verbindungen z. B. HTTPS-Verbindungen, welche rein zur Administration oder Konfiguration des Terminals bestimmt sind (siehe 3.6.6).

Es ist eine beidseitige Authentisierung zwischen Server (d.h. dem Kartenterminal) und Client (d.h. Konnektor) umzusetzen, bei der geprüft werden MUSS, ob der Client ein betriebszugelassener Konnektor ist und ob der Server ein betriebszugelassenes[18] und gepairtes Kartenterminal ist.

Komponentenzertifikate für Konnektoren werden durch so genannte Trusted Service Provider für Komponentenzertifikate Konnektoren (TSP-K) ausgestellt. Jedes Komponentenzertifikat eines Konnektors kann auf ein CA-Zertifikat innerhalb der Trusted Component List (TCL) zurückgeführt werden. Da das Kartenterminal nicht die gesamte TCL speichern kann MUSS es mindestens die CA-Zertifikate der TSP-K speichern (z. B. in der Firmware). Beim Einbringen dieser CA-Zertifikate in das Kartenterminal und ihrer anschließenden Speicherung innerhalb des Kartenterminals MUSS deren Authentizität gewährleistet werden. Nehmen neue CAs ihren Betrieb für das Generieren von Komponentenzertifikaten für Konnektoren auf, MÜSSEN die zugehörigen CA-Zertifikate in ein eHealth-Kartenterminal eingebracht werden können. Dies KANN zum Beispiel über einen Update der Firmware des Kartenterminals erfolgen (siehe auch [gemPKI_KT#7.1.1]).

[17] Ein Wechsel des Schlüsselmaterials ist damit über die Einbeziehung einer neuen Schlüsselgeneration in die Firmware möglich. Auch ist es zulässig (und sogar empfohlen), dass eine Firmware nur die öffentlichen Schlüssel einer übergeordneten CA enthält und das konkrete Zertifikat zur Signatur in das bzw. an das Signaturenvelope ein- bzw. angefügt wird.

[18] Die Bauartzulassung des Kartenterminals wird organisatorisch abgebildet, indem die Inbetriebnahme eines Kartenterminals durch einen Administrator erfolgt, welcher die Integrität und Authentizität des Terminals im Rahmen des Pairings prüft.

Zur Feststellung, ob das ansteuernde System ein betriebszugelassener Konnektor[19] ist, MUSS das Kartenterminal im Zuge des TLS-Verbindungsaufbaus das vom Konnektor präsentierte Zertifikat gemäß [gemPKI_KT#7.1.2] prüfen. Die Prüfung erfolgt immer einstufig, d. h. das präsentierte Zertifikat lässt sich direkt anhand eines am Kartenterminal hinterlegten CA-Zertifikates prüfen. Verfügt das Kartenterminal nicht über Pairinginformationen oder ist der öffentliche Schlüssel des präsentierten Zertifikats nicht in diesen enthalten, akzeptiert es den Verbindungsaufbau, DARF jedoch SICCT bzw. EHEALTH Kommandos, die nicht in Kapitel 4.11.1 angeführt sind, NICHT ausführen. Ist der öffentliche Schlüssel in einem Pairingblock enthalten, akzeptiert das Kartenterminal alle SICCT und EHEALTH Befehle. In dieser Phase wird das korrekte Shared Secret nur durch den Konnektor geprüft. (Durch einen folgenden Aufruf von EHEALH TERMINAL AUTHENTICATE mit P2=02). Das KT selbst bleibt passiv.

Damit der Konnektor die KT-Identität überprüfen kann, präsentiert das Terminal sein SMKT-Zertifikat (C.SMKT.AUT) dem Client im Rahmen des TLS-Verbindungsaufbaus. Der Konnektor prüft gemäß [gemPKI_KT#7.2.2], ob es sich um ein gültiges SMKT-Komponentenzertifikat handelt und ob ihm das vom Kartenterminal präsentierte Zertifikat durch ein Pairing bekannt gemacht wurde. Handelt es sich nicht um ein gültiges SMKT-Komponentenzertifikat wird der TLS-Verbindungsaufbau abgebrochen. Ist das Zertifikat ein gültiges SMKT-Komponentenzertifikat welches jedoch noch nicht mittels Pairing am Konnektor bekannt gemacht wurde, akzeptiert der Konnektor die TLS-Verbindung, jedoch stuft er das Kartenterminal als nicht vertrauenswürdig ein und führt nur jene SICCT und EHEALTH Kommandos aus, die in Kapitel 4.11.1 angeführt sind. Sind beide Prüfungen erfolgreich, wird die TLS-Verbindung akzeptiert. Der TLS-Verbindungsaufbau ist nach diesem Schritt abgeschlossen.

Ist für das Kartenterminalzertifikat am Konnektor eine Pairinginformation vorhanden, so prüft der Konnektor nach erfolgtem TLS Aufbau die Pairinginformation (siehe Kapitel 3.7.2.2). Schlägt diese Prüfung fehl, wird die Verbindung abgebrochen.

4.11.1 Positiv Liste für Kommandos ohne gültige Pairinginformation

Folgende Kommandos MÜSSEN nach dem TLS-Verbindungsaufbau unabhängig vom Stand des Pairings am Kartenterminal möglich sein (das Pairing wird in Kapitel 3.7.2 beschrieben), um das Kartenterminal in Betrieb zu nehmen, bzw. um ein Firmwareupdate zu ermöglichen und Statusinformationen abzufragen. Andere SICCT- oder EHEALTH-Kommandos als diese DÜRFEN NICHT ausgeführt werden, falls der öffentliche Schlüssel des beim TLS-Verbindungsaufbau präsentierten Konnektorzertifikats nicht in den Pairinginformationen des Kartenterminals enthalten ist:

- EHEALTH TERMINAL AUTHENTICATE
- SICCT CT INIT CT SESSION
- SICCT CT CLOSE CT SESSION
- SICCT GET STATUS

[19] Für eine automatische Prüfung der Betriebszulassung eines Konnektors durch andere IT-Systeme steht ein X509-Zertifikat zusammen mit den damit verbundenen geheimen und öffentlichen Schlüsseln im Rahmen der Identitäten des Konnektors zur Verfügung. Es ist dabei durch organisatorische Prozesse im Rahmen der Baureihenzulassung sichergestellt, dass nur betriebszugelassene Geräte mit solchen Zertifikaten ausgestattet werden.

- SICCT CT DOWNLOAD INIT
- SICCT CT DOWNLOAD DATA
- SICCT CT DOWNLOAD FINISH
- SICCT SELECT CT MODE

4.12 Abbau der SICCT-spezifischen TLS-Verbindung

Wird die nach [SICCT#6.3.1.1] spezifizierte SICCT-spezifischen TLS-Verbindung, die zur Nutzung für eine Kommunikation gemäß SICCT-Protokoll vorgesehen ist, beendet, MUSS das Kartenterminal alle in ihm gesteckten Karten inklusive eventuell vorhandener SMCs resetten, sowie eventuell erlangte Sicherheitszustände verlieren.

4.13 Auslieferungszustand

Ein spezifikationskonformes eHealth-Kartenterminal darf im Auslieferungszustand nur SICCT-Verbindungen über TLS akzeptieren Dies gilt ergänzend zu den Festlegungen zum Auslieferungszustand in Abschnitt 6.1.5 der SICCT-Spezifikation („Auslieferungszustand“).

1 Anhang

2 A1 - Abkürzungen

Kürzel	Erläuterung
AES	Advanced Encryption Standard
BDSG	Bundesdatenschutzgesetz
BNetzA	Bundesnetzagentur
CA	Certificate Authotrity
CEN	Comité Européen de Normalisation
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
eGK	elektronische Gesundheitskarte
EMV	Europay Mastercard Visa
IEC	International Electrotechnical Commission
ISO	International Standardization Organization
HBA	Heilberufeausweis, siehe auch HPC
HPC	Health Professional Card
KT	Kartenterminal
KVK	Krankenversicherungskarte
LAN	Local Area Network
MAC	Message Authentication Code
MAC-Adresse	Media Access Control Adresse
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
SigG	Signaturgesetz
SigV	Signaturverordnung
SICCT	Secure Interoperable ChipCard Terminal
SM-KT	Security-Modul-Kartenterminal
TCL	Trusted Component List
TSP-K	Trusted Service Provider Komponentenzertifikate Konnektor
TLS	Transport Layer Security

Kürzel	Erläuterung
TCP/IP	Transmission Control Protocol over Internet Protocol
VerSA	Verteilte Signatur Arbeitsplätze

1 A2 - Glossar

2 Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt [GLOSSAR].

3 A3 - Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[CEN ENV]	CEN ENV1375-1 (1994): Identification card systems - Intersector integrated circuit(s) card additional formats – Part 1: ID-000 card size and physical characteristics
[gemSpec_eGK_P2]	gematik (20.12.2007): Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte ; Teil 2 – Anwendungen und anwendungsspezifische Strukturen Version 2.1.0, www.gematik.de
[gemSpec_Kon]	gematik (26.03.2008): Einführung der Gesundheitskarte - Konnektorspezifikation; Version 2.6.0, www.gematik.de
[gemSpec_Krypt]	gematik (26.03.2008): Einführung der Gesundheitskarte - Verwendung Kryptographischer Algorithmen in der Telematikinfrastruktur Version 1.3.0 Kap. 5.1.1.4 X.509 TLS/SSL-Zertifikate Kap. 5.2 Zufallszahlengeneratoren Kap. 6.4.2 SSL/TLS-Kontext
[gemPKI_KT]	gematik (26.03.2008): Einführung der Gesundheitskarte - PKI für die X.509-Zertifikate der Identitäten der eHealth-Kartenterminals – Lastenheft Version 1.0.0
[gemZulKomp-KT]	gematik (06.06.2007): Einführung der Gesundheitskarte - Zulassung von dezentalen IT-Komponenten in der Telematikinfrastruktur (Kartenterminal) Version 1.0.0
[gemSiKo]	gematik (10.03.2008): Einführung der Gesundheitskarte - Übergreifendes Sicherheitskonzept der Telematikinfrastruktur Version 2.2.0

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-PP-0032]	BSI (in Vorbereitung): Common Criteria Schutzprofil (Protection Profile) für ein Kartenterminal im elektronischen Gesundheitswesen BSI-0032-2007.
[EMV_41]	EMVCo (Mai 2004): EMV Integrated Circuit Card Specifications for Payment Systems Book 1: Application Independent ICC to Terminal Interface Requirements, Version 4.1
[GLOSSAR]	gematik (15.02.2008): Einführung der Gesundheitskarte - Projektglossar Version 2.2.0, www.gematik.de
[HPC-P1]	Bundesärztekammer et al. (in Vorbereitung): German Health Professional Card and Security Module Card Part 1: Commands, Algorithms and Functions of the COS Platform Version 2.x.x
[HPC-P3]	Bundesärztekammer et al. (in Vorbereitung): German Health Professional Card and Security Module Card Part 3: SMC Applications and Functions Version 2.x.x
[BÄK_POL]	Bundesärztekammer (03.03.2006/08.02.2006): Die „Gemeinsame Policy“ für die Herausgabe der HPC ist ein gemeinsames Dokument der Bundesärztekammer, der Bundeszahnärztekammer, der WUV der Apotheker, der Bundespsychotherapeutenkammer und der Kassenzahnärztlichen Bundesvereinigung. Das Dokument inkl. Anlage zum Gültigkeitsmodell V0.9.3; Rechtliches Niveau und rechtliche Einordnung der ausgestellten Zertifikate sowie Anhang zum Gültigkeitsmodell (Kompromissmodell) gehört nicht zur „Gemeinsamen Policy“ und ist ein Dokument der BÄK.
[BSI-M2.11]	BSI (Oktober 2007): IT-Grundschutzkataloge – Maßnahmenkatalog Organisation (9. Ergänzungslieferung) http://www.bsi.bund.de/gshb/deutsch/m/m02011.htm
[ISO7810]	ISO/IEC 7810: 2003 Identification cards - Physical characteristics
[ISO7816-10]	ISO/IEC 7816-10 (1999): Identification cards - Integrated circuit(s) cards with contacts Part 10 - Electronic signals and answer to reset for synchronous cards
[ISO7816-2]	ISO/IEC 7816-2 (1999): Identification cards - Integrated circuit(s) cards with contacts Part 2 - Dimensions and location of the contacts

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ISO7816-3]	ISO/IEC 7816-3 (1997): Identification cards - Integrated circuit(s) cards with contacts Part 3 - Electronic signals and transmission protocols
[ISO9796-2]	Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms Second edition, 2002-10-01
[KVK]	Technische Spezifikation der Versichertenkarte, 2004, Version: 2.05
[PKCS #1]	PKCS #1 v2.1 (14.6.2002): RSA Cryptography Standard, RSA Laboratories, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf
[RFC2119]	RFC 2119 (March1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt
[RC2246]	RFC2246 (Januar 1999): The TLS Protocol, Version 1.0 http://www.ietf.org/rfc/rfc2246.txt
[RFC3546]	RFC3546 (Juni 2003): Transport Layer Security (TLS) Extensions http://www.ietf.org/rfc/rfc3546.txt
[RFC 4346]	RFC 4346 (April 2006): The Transport Layer Security (TLS) Protocol Version 1.1 http://www.ietf.org/rfc/rfc4346.txt
[SICCT]	SICCT (19.11.2007): TeleTrusT, SICCT Secure Interoperable ChipCard Terminal, Version 1.20
[SigÄndG]	Bundesgesetzblatt Nr. 1, S.2 (2005): 1. Gesetz zur Änderung des Signaturgesetzes
[SigG01]	Bundesgesetzblatt Nr. 22 S.876 (2001): Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften),
[SigV01]	Bundesgesetzblatt Nr. 509, S. 3074 (2001): Verordnung zur elektronischen Signatur – SigV
[SP800-22]	National Institute of Standards and Technology (2001); A statistical test suite for random and pseudorandom number generators for cryptographic applications NIST Special Publication 800-22

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[TR-3120]	BSI (23.10.2007): TR-3120 Technische Richtlinie zur Kartenterminalidentität Version 1.0

A4 – Offene Punkte

Eine Reihe von Punkten muss bis zum Abschluss von Anwendertests offen bleiben, da die Erfahrungen und Rückmeldungen aus dem Feld für endgültige Festlegungen ausschlaggebend sind.

Die Anforderungen und Details zur Umsetzung des Transparenten Kanals vom Konnektor zum Kartenterminal stehen noch aus.

Die Anforderungen und Details zur Umsetzung eines gematik-Prüfsiegels stehen noch aus.

Die Anforderungen und Details zur Umsetzung von Mehrwertdiensten, welche ein Kartenterminal anbietet, stehen noch aus und werden in Release 3 behandelt.

Die maximal zulässige Dauer des Pollingintervalls zur Überprüfung des Vorhandenseins des SM-KT steht noch aus.