gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation eHealth-Kartenterminal

Version:	3.11.0
Revision:	167345
Stand:	02.10.2019
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_KT

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

Dokumentenhistorie

Version	Stand	Kap.	Grund der Änderung, besondere Hinweise	Bearbeitung
2.6.0	26.03.08		Freigegeben Grundlage für den Basis-Rollout und veröffentlicht mit Rel. 0.5.2 bzw. 0.5.3	gematik
2.8.0	15.09.09		Freigegeben Festgelegt im Rahmen der [TestV]	gematik
2.8.1	15.03.10		Modellierungstechnische Überarbeitung Einarbeitung der SRQs: • Streichung EHEALTH • Streichung Kommando aus Positivliste • DF.KT Zugriff Überarbeitung Kapitel 3.6.9	SPE/DK
3.0.0	15.10.12		Überarbeitung im Rahmen von P71 Basis TI 1 • Streichung CT MODE • Einschränkung CMD DO • Anpassung DF.KT Zugriff • Werksreset über PUK • Aufnahme von PKI-Bestandteilen • Ausgliederung des Firmware-Gruppen Konzeptes • Aufnahme „physikalische Sicherheit“ • Formelle Überarbeitung	ITS/SPE
3.1.0	12.11.12		freigegeben	gematik
3.2.0	06.06.13		Einarbeitung Gesellschafterkommentare, Bieterfragen und interner Kommentare	P77
3.3.0	15.08.13		Einarbeitung lt. Änderungsliste vom 08.08.13	P77

3.4.0	21.02.14		Losübergreifende Synchronisation	PL P77
3.5.0	17.06.14		Streichung SMC-B als Trägerkarte des DF.KT gemäß P11-Änderungsliste	P77
3.6.0	24.08.16		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik
3.7.0	28.10.16		Aufnahme SMC-B für Organisationen der Gesellschafter, Anpassungen gemäß Änderungsliste	
3.7.1	13.02.17		Änderungen bzgl. eIDAS, Streichung SigG/SigV	gematik
3.8.0	21.04.17		Anpassungen lt. Änderungsliste	gematik
3.9.0	14.05.18		Anpassungen auf Grundlage von P15.4	gematik
3.10.0	15.05.19		Anpassungen lt. Änderungsliste P18.1	gematik
			Anpassungen lt. Änderungsliste P20.1	gematik
3.11.0	02.10.19		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes 7
1.1 Zielsetzung 7
1.2 Zielgruppe 7
1.3 Geltungsbereich 7
1.4 Abgrenzung 8
1.5 Methodik 8
2 Architektur 9
2.1 Anschlussarten eines Terminals 11
2.2 Zulassungsverfahren, Zertifikat 12
2.3 Allgemeine Anforderungen 12
2.3.1 Unterstützung Prozessor- und Speicherkarten 12
2.3.2 Anforderungen an die Kartenterminals 12
2.3.3 Benutzerführung 13
2.3.4 Performance 13
2.3.5 Zuverlässigkeit 14
2.3.6 Stromversorgung 14
2.3.7 Fehlertoleranz 15
2.3.8 Wartbarkeit 15
2.3.9 Gehäuse 15
2.3.9.1 Aufbringen der MAC-Adresse 15
2.3.9.2 Aufbringen eines Prüfzeichens 16
2.3.10 Kommunikationsprotokolle 17
2.3.11 Firmware Update 17
2.3.12 Terminal Managementverfahren 18
2.3.12.1 Anzeige des SICCT-Terminalnamens 19
2.3.12.2 Produkttypversion und Selbstauskunft 20
2.3.13 Mehrwertmodule 20
2.3.14 Zugriffsanzeige 21
2.3.15 Desinfektion der Kartenterminals (informativ) 21
2.3.16 Produktsicherheit (informativ) 21
2.3.17 Physikalische Sicherheit-Klima 22
2.3.18 Physikalische Sicherheit-Vibration 22
2.3.19 Benutzerfreundlichkeit und weitere Kennwort-/PIN-Eingaben 23
2.4 Spezielle sicherheitstechnische Anforderungen 23
2.4.1 Firmware Update 24
2.4.1.1 Konzept der Firmware-Gruppen 25
2.4.2 Anzeige des vertrauenswürdigen Zustands 25
2.4.3 Sicherer PIN-Modus 25
2.4.4 Sicherheitsanforderungen LAN-gekoppelter Terminals 26
2.4.5 Terminal Managementverfahren 26

2.4.5.1 Sicherung der administrativen TLS-Verbindung 27
2.4.5.2 Anforderungen an Kennwörter zur Sicherung der Managementschnittstelle 29
2.4.5.3 Anforderungen an die PUK für die Durchführung des Werksresets 31
2.4.6 Übergreifende Sicherheitsanforderungen 32
2.4.7 Protection Profile (Schutzprofil) 33
2.4.7.1 Umgebungsanforderungen für Kartenterminals 33
2.4.8 Zufallszahlen und Schlüssel 33

2.5 Festlegungen zu Kartenterminalidentität und Schlüsselmanagement 34
2.5.1 Anforderungen an die Kartenterminalidentität 37
2.5.1.1 Ausführung 37
2.5.1.2 Bedeutung für das Kartenterminal 38
2.5.1.3 Produktion und Auslieferung 38
2.5.2 Pairing zwischen Konnektor und eHealth-Kartenterminal 38
2.5.2.1 Initiales Pairing 40
2.5.2.2 Überprüfung der Pairing-Information durch einen Konnektor 43
2.5.2.3 Pairing-Informationen bei Außerbetriebnahme 44
2.5.2.4 Wartungs-Pairing 44

3 Spezielle technische Anforderungen 47

3.1 Abgeleitete mechanische Anforderungen 47
3.1.1 Kartentypen 47
3.1.2 Kontaktiereinheiten 47
3.1.2.1 ID-1 Kartenkontaktierungen 48
3.1.2.2 ID-000-Kartenkontaktierungen 49
3.1.3 Bauformen 50

3.2 Abgeleitete elektrische Anforderungen 50
3.2.1 Elektrische Anforderungen für kontaktbehaftete Karten 50
3.2.2 Reset-Verhalten und ATR-Bearbeitung 50

3.3 Transport von Zeichen 51

3.4 Chipkartenprotokolle 51

3.5 Isolation von Verbindungen zum Kartenterminal 52

3.6 Gleichzeitige Verbindungen zum Kartenterminal 53

3.7 Kartenterminalkommandos 54
3.7.1 Verbindlichkeit des SICCT-Kommandos CONTROL COMMAND 54
3.7.2 Command EHEALTH TERMINAL AUTHENTICATE 54
3.7.2.1 Funktion 55
3.7.2.2 Der Zustand EHEALTH EXPECT CHALLENGE RESPONSE 65
3.7.2.3 Anwendungsbedingungen 66
3.7.2.4 Command Structure 66
3.7.2.5 Response Structure 69
3.7.2.6 Status-Codes SW1-SW2 69
3.7.2.7 Shared Secret Data Object 70
3.7.2.8 Shared Secret Challenge Data Object 71
3.7.2.9 Shared Secret Response Data Object 71
3.7.3 Ergänzung der Commands SICCT OUTPUT und SICCT INPUT 72
3.7.4 Ergänzung der Commands SICCT REQUEST ICC und SICCT EJECT ICC ... 72

3.7.5 Ergänzung des Command SICCT PERFORM VERIFICATION....72
3.7.6 Ergänzung des Command SICCT MODIFY VERIFICATION DATA....73
3.7.7 Änderungen des Card Terminal Manufacturer Data Objects....74
3.7.8 Ergänzung zu Service Discovery/Announcement....76
3.7.9 Ergänzung des Command SICCT INIT CT SESSION....76
3.7.10 Verbindlichkeit des SICCT-Kommandos SICCT SELECT CT MODE....77
3.7.11 Einschränkung des Command-To-Perform Data Objects....77
3.8 Verhalten bei der PIN-Eingabe....77
3.9 Festlegungen zur Sicherung der Firmware Updates....79
3.10 Auswahl kryptographischer Algorithmen für TLS....79
3.11 Authentisierung beim Aufbau der SICCT-spezifischen TLS-Verbindungen..80
3.11.1 Positivliste für Kommandos ohne gültiges Konnektorzertifikat....85
3.11.2 Positivliste für Kommandos ohne gültige Pairing-Information....86
3.12 Abbau der SICCT-spezifischen TLS-Verbindung....87
3.13 Auslieferungszustand....87
3.14 Werksreset....88
4 Anhang A - Verzeichnisse....91
4.1 Abkürzungen....91
4.2 Glossar....92
4.3 Tabellenverzeichnis....92
4.4 Abbildungsverzeichnis....93
4.5 Referenzierte Dokumente....93
4.5.1 Dokumente der gematik....93
4.5.2 Weitere Dokumente....95

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert Anforderungen für eHealth-Kartenterminals, die bei der Realisierung (bzw. dem Betrieb) von Produkttypen der TI zu beachten sind. Diese Anforderungen sind als übergreifende Regelungen relevant für Interoperabilität und Verfahrenssicherheit.

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

Es beschreibt besondere funktionale Anforderungen an ein eHealth-Kartenterminal, gibt besondere sicherheitstechnische Anforderungen vor und beschreibt technisch notwendige Maßnahmen insbesondere für eine Nutzung von neuen Diensten der Telematikinfrastruktur für das Gesundheitswesen auf Basis der eGK.

1.2 Zielgruppe

Das Dokument ist maßgeblich für Hersteller von eHealth-Kartenterminals sowie Hersteller von Produkttypen, die hierzu eine Schnittstelle besitzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzung

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.

Festlegungen, welche im Schutzprofil (Protection Profile) des Kartenterminals gemäß Common Criteria getroffen werden, werden hier nur angeführt, soweit es für das Verständnis erforderlich ist.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>
Text / Beschreibung
[<=**]**

Dabei umfasst die Anforderung sämtliche innerhalb Afo-ID und der Textmarke angeführten Inhalte.

In dieser Spezifikation wird der Begriff „Administrator“ verwendet. Hierunter ist keine Berufsbezeichnung zu verstehen, sondern die Rolle Administrator, welche zur Verwaltung der Komponente besondere Rechte und Aufgaben hat. Darüber, welche Person diese Rolle ausfüllt, werden keine Vorgaben gemacht.

2 Architektur

Ein eHealth-Kartenterminal für den Einsatz im deutschen Gesundheitswesen basiert auf der Spezifikation SICCT [SICCT], welche durch Profilierungen für den Betrieb als eHealth-Kartenterminal mit dieser Spezifikation angepasst wird.

Die Ableitungen der physischen Ausprägungen der einzelnen Kartenterminaltypen sind informativ in Abbildung „Pic_KT_0004 Physische Ausprägung Kartenterminal“ basierend auf dem Architekturmodell der SICCT-Spezifikation [SICCT#3.2] dargestellt.

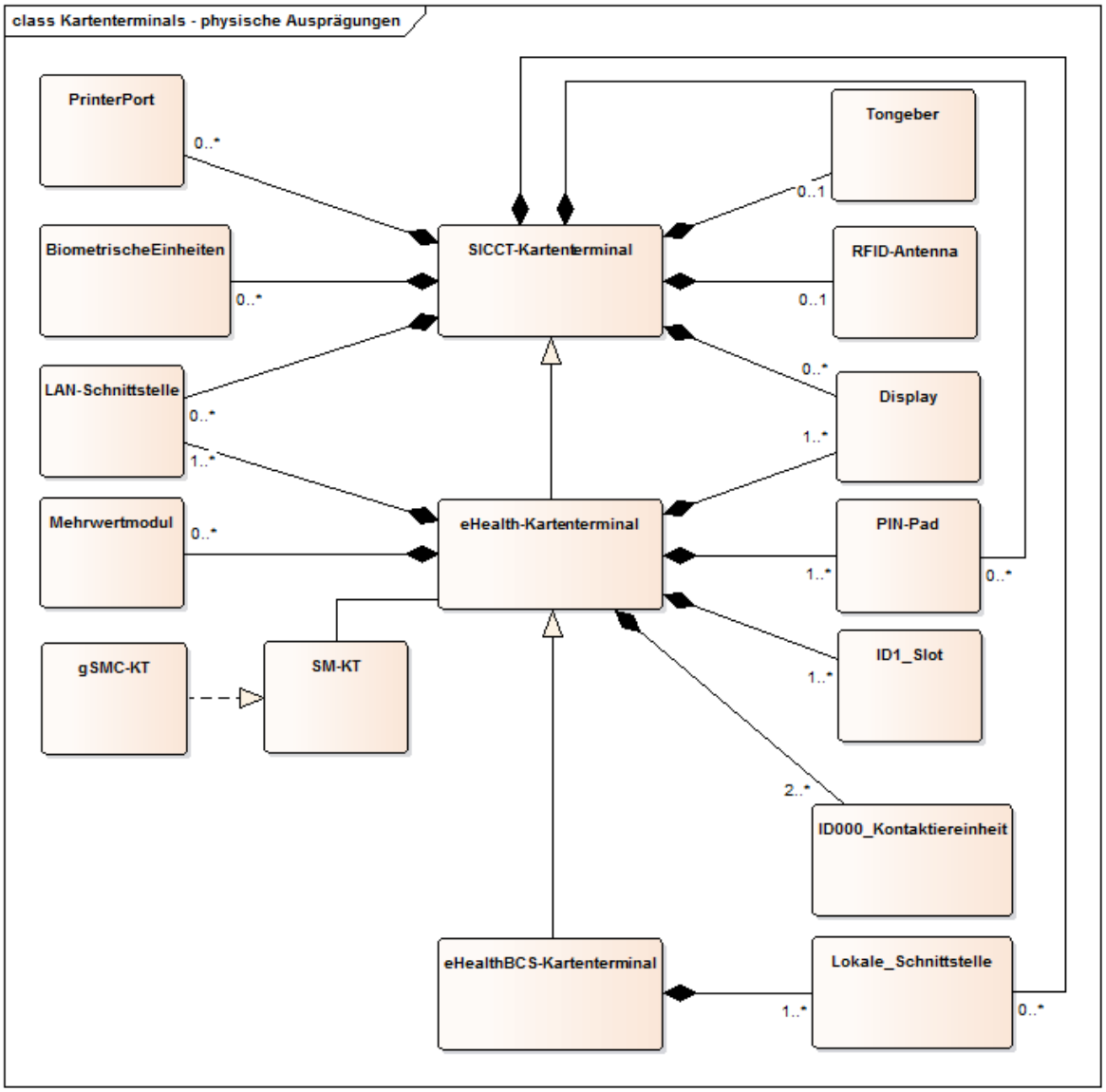


Abbildung 1: Pic_KT_0004 Physische Ausprägung Kartenterminal

Für die physische Ausprägung profiliert diese Spezifikation den SICCT-Standard dahingehend, dass das eHealth-Kartenterminal ein PIN-Pad und ein Display verbindlich

aufweisen muss. Ebenso werden für das eHealth-Kartenterminal mindestens eine ID-1 und mindestens zwei ID-000-Kontaktiereinheiten gefordert.

Das eHealth-Kartenterminal muss u. a. zur Authentisierung, zur Integritätssicherung und zur Sicherstellung der Vertraulichkeit der über die LAN-Schnittstelle übertragenen Daten mit einem kryptographischen Schlüssel arbeiten. Für diesen Schlüssel ist aufgrund des teilweise sehr hohen Schutzbedarfes der über die LAN-Schnittstelle übertragenen Informationsobjekte ein sicherer Schlüsselspeicher, ein SM-KT, erforderlich. eHealth-Kartenterminals müssen als physische Ausprägungen der SM-KT die gSMC-KT unterstützen.

Für die Anbindung des eHealth-Kartenterminals an einen Konnektor über die LAN-Schnittstelle ist das SICCT-Protokoll mit den EHEALTH-Erweiterungen (siehe Kapitel 3.7) verpflichtend vorgeschrieben.

Die sich durch die Spezifikation des eHealth-Kartenterminals ergebenden Schnittstellen und die sie nutzenden Kommunikationspartner sind im Komponentendiagramm informativ zusammenfassend dargestellt (siehe Abbildung „Pic_KT_0006 Schnittstellen des Kartenterminals“).

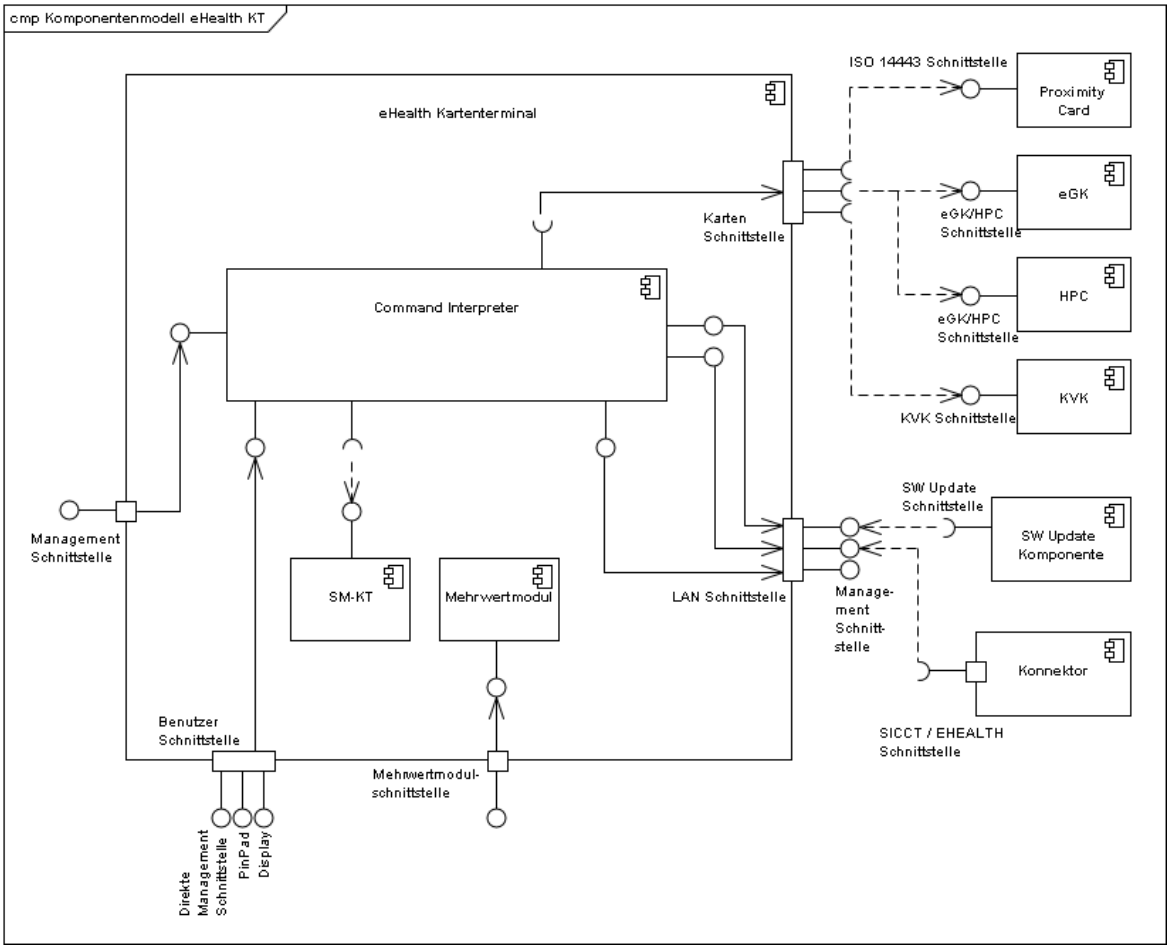


Abbildung 2: Pic_KT_0006 Schnittstellen des Kartenterminals

TIP1-A_2948 - Definition SICCT/eHealth
Das eHealth-Kartenterminal MUSS die SICCT-Spezifikation [SICCT] umsetzen, soweit diese nicht durch die Spezifikation des eHealth-Kartenterminals [gemSpec_KT] eingeschränkt bzw. erweitert wird.
[<=]

2.1 Anschlussarten eines Terminals

Die konkrete Ausprägung 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 grundsätzlich zwei unterschiedliche Lösungsansätze zur Realisierung der Anforderungen dieser Spezifikation umgesetzt werden können:

- **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, muss der Hersteller der gematik gegebenenfalls technischen Support leisten. Die vorliegende Spezifikation ist in diesen Fällen direkt vom Kartenterminal zu erfüllen und nur das Kartenterminal stellt einen Prüf- und Evaluationsgegenstand (Prüf- und Evaluierungsgegenstand im Sinne einer Sicherheitszertifizierung und der Zulassung durch die gematik gemäß [gemZulKomp_KT]) 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 kann dabei auf einem anderen Gerät ablaufen 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 (z. B. Kabel im Sichtbereich des Nutzers) 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 (Prüf- und Evaluierungsgegenstand im Sinne einer Sicherheitszertifizierung und der Zulassung durch die gematik gemäß [gemZulKomp_KT]).

2.2 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 [gemZul_KT].

TIP1-A_2949 - Zulassungsrichtlinien für virtuelle und netzwerkfähige Kartenterminals
Das eHealth-Kartenterminal MUSS unabhängig von seiner Realisierung (z. B. als virtuelles oder netzwerkfähiges eHealth-Kartenterminal) dieselben Zulassungsrichtlinien erfüllen (siehe [gemZul_KT]).
[<=**]**

2.3 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 bzw. bei den Organisationen des Gesundheitswesens (z.B. Leistungserbringerorganisationen und Kostenträgerorganisationen) beschrieben.

2.3.1 Unterstützung Prozessor- und Speicherkarten

Das eHealth-Kartenterminal muss die durch die Telematikinfrastruktur entstehenden Anwendungsfälle unter Nutzung von Prozessorkarten sowie Speicherkarten (KVK) unterstützen.

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 spezifikations- und norm-konformer HBAs,
- Verarbeitung spezifikations- und norm-konformer SMCs,
- Verarbeitung spezifikations- und norm-konformer ZOD-Karten und
- Verarbeitung spezifikations- und norm-konformer HBA-qSig-Karten

2.3.2 Anforderungen an die Kartenterminals

eHealth-Kartenterminals müssen aus Gesamtsystemsicht einem Konnektor folgende Funktionen 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 Event-Mechanismus zur Meldung an den Konnektor (zur Vermeidung von Polling),
- eine authentisierte, verschlüsselte und integritätsgesicherte Kommunikation,
- eine eindeutige, kryptographische Identität in einem „sicheren“ Schlüsselspeicher bereitstellen, für den gilt, dass die Schlüssel nicht durch einen Angreifer aus dem Gerät auslesbar sein dürfen (siehe Kapitel 2.5).

2.3.3 Benutzerführung

TIP1-A_3106 - Benutzerführung und integriertes Display
Das eHealth-Kartenterminal MUSS zur Benutzerführung über ein integriertes Display verfügen.
[<=]

TIP1-A_2950 - Mindestanforderung Display des eHealth-Kartenterminals
Das eHealth-Kartenterminal MUSS über ein Display verfügen, mit dem mindestens zwei Zeilen à 16 Zeichen als ASCII-Text dargestellt werden kann.
[<=]

TIP1-A_3034 - Display eines eHealth-Kartenterminals
Das eHealth-Kartenterminal KANN über die Anforderung [TIP1-A_2950] hinaus zur Anzeige ein Display implementieren, welches mehr als zwei Zeilen a 16 Zeichen ASCII-Text unterstützt.
[<=]

Graphische Displays, die in der Lage sind zwei Zeilen anzuzeigen, sind zugelassen.

TIP1-A_2951 - eHealth-Kartenterminal: Eingabeeinheit
Das eHealth Kartenterminal MUSS zur Eingabe einer PIN und zur damit verbundenen Authentisierung des Nutzers ein Tastenfeld oder eine vergleichbare Eingabemöglichkeit für eine numerische PIN besitzen.
[<=]

TIP1-A_2952 - eHealth-Kartenterminal: weitere Sensoren
Das eHealth-Kartenterminal KANN zusätzlich zu Display und PIN-Pad weitere Sensoren und Eingabeeinheiten vorsehen.
[<=]

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

2.3.4 Performance

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 (im Sinne von [SICCT], [eGK], [HBA]) unterstützt.

TIP1-A_3110 - Gleichzeitige Kommunikation zu unterschiedlichen Karten
Das eHealth-Kartenterminal SOLL eine gleichzeitige Kommunikation zu unterschiedlichen Karten parallel abarbeiten.
[<=]

Bzgl. der Geschwindigkeit für die Kommunikation zwischen Kartenterminal und Karte ist hier Kap. 3.2.2 zu beachten. Die weiteren Vorgaben zur Performance werden im Dokument [gemSpec_Perf] erhoben.

2.3.5 Zuverlässigkeit

TIP1-A_3035 - Zuverlässigkeit des eHealth-Kartenterminals im Betrieb
Das eHealth-Kartenterminal MUSS eine Zuverlässigkeit im Betrieb (im Sinne der Mean-Time-Between-Failure bei Rund-um-die-Uhr-Betrieb) von mindestens
3 Jahren bzw. 200.000 Steckzyklen gewährleisten.
[<=]

TIP1-A_2953 - Zuverlässigkeitsprognose eHealth-Kartenterminals
Der Hersteller des eHealth-Kartenterminals MUSS eine Zuverlässigkeitsprognose seines eHealth-Kartenterminals mit Darstellung der zugrunde gelegten Ausfallraten und Stückzahlen der Bauelemente und der anderen zuverlässigkeitsrelevanten Elemente (Lötstellen, Leiterbahnen, etc.) bereitstellen.
[<=]

TIP1-A_2954 - Zuverlässigkeitsprognose eHealth-Kartenterminal
Der Hersteller des eHealth-Kartenterminals MUSS die Zuverlässigkeitsprognose nach [TIP1-A_2953] seines eHealth-Kartenterminals nachvollziehbar darstellen und Schätzungen erläutern.
[<=]

2.3.6 Stromversorgung

TIP1-A_3942 - Belastbarkeit des Netzteils
Der Hersteller des eHealth-Kartenterminals MUSS sicherstellen, dass das Netzteil des eHealth-Kartenterminals so beschaffen ist, dass ein Dauerbetrieb von 24 Stunden pro Tag möglich ist, ohne dass eine Einschränkung der Funktionsfähigkeit zu verzeichnen ist.
[<=]

Zum Nachweis der Belastbarkeit im Dauerbetrieb sind Berechnungen zulässig.

TIP1-A_2955 - Dauerhafte Stromversorgung der im eHealth-Kartenterminal gesteckten Chipkarte(n)
Das eHealth-Kartenterminal MUSS eine dauerhafte Stromversorgung der im eHealth-Kartenterminal gesteckten Chipkarte(n) mit dem Maximalstrom nach den derzeit gültigen internationalen Standards ([ISO7816-3] und [EMV_41]) gewährleisten, sobald die Chipkarte(n) gesteckt sind.
[<=]

TIP1-A_2956 - Kurzzeitig höherer Strombedarf von Chipkarten (Spike)
Das eHealth-Kartenterminal MUSS auch bei kurzzeitig höherem Strombedarf der Chipkarten (siehe [SICCT#A1]) in jedem Fall gewährleisten, dass die Funktionsfähigkeit des eHealth-Kartenterminals und die Stromversorgung der im eHealth-Kartenterminal

gesteckten Chipkarten erhalten bleibt.
[<=]

2.3.7 Fehlertoleranz

TIP1-A_3111 - Transiente bzw. überbrückbare Fehlerzustände bei der Kartenkommunikation
Das eHealth-Kartenterminal MUSS transiente bzw. überbrückbare Fehlerzustände gemäß der Kartenspezifikationen bei der Kartenkommunikation erkennen und automatisch bereinigen.
[<=]

Konkret, aber nicht ausschließlich bezieht sich dies auf die Resynchronisation der Kartenkommunikation.

TIP1-A_2957 - Behandlung Bedienungsfehler und ungültige Eingaben
Das eHealth-Kartenterminal MUSS Bedienungsfehler und ungültige Eingaben am Display des eHealth-Kartenterminals signalisieren oder ignorieren.
[<=]

2.3.8 Wartbarkeit

Der Hersteller sei darauf hingewiesen, dass aufgrund der besonderen Sicherheitsanforderungen (Sicherheitssiegel), die keine Öffnung des Gerätes zu Wartungszwecken ermöglichen, der wartungsfreie Betrieb, bis auf das Einspielen von Firmware-Updates, sicherzustellen ist.

2.3.9 Gehäuse

2.3.9.1 Aufbringen der MAC-Adresse

TIP1-A_2958 - Sichtbarkeit MAC-Adresse des eHealth-Kartenterminals
Das eHealth-Kartenterminal MUSS die MAC-Adresse über mindestens eine der zwei folgenden Varianten dem Nutzer sichtbar machen:
Variante 1) Die MAC-Adresse MUSS gut erkennbar und in nicht unbeschadet ablösbarer Form (d. h. die MAC-Adresse darf nicht nach dem Entfernen auf ein anderes Gerät aufgebracht werden können) auf dem Gehäuse aufgebracht (z. B. geklebt, gedruckt oder geprägt) sein.
Variante 2) Die MAC-Adresse MUSS über eine lokale Terminalfunktion abrufbar sein. (z. B. auf dem Display).
[<=]

TIP1-A_2959 - Lokale Terminalfunktion zur Anzeige der MAC-Adresse
Wird die MAC-Adresse des eHealth-Kartenterminals nach [TIP1-A_2958] über eine lokale Terminalfunktion zur Anzeige gebracht, dann MUSS das eHealth-Kartenterminal diese Funktion zur Verfügung stellen, solange keine SICCT-Session am Kartenterminal aktiv ist.
[<=]

TIP1-A_2960 - Unabhängigkeit Netzwerkanschluss bei lokaler Terminalfunktion zur Anzeige der MAC-Adresse
Wird die MAC-Adresse des eHealth-Kartenterminals nach [TIP1-A_2958] über eine lokale Terminalfunktion zur Anzeige gebracht, so MUSS das eHealth-Kartenterminal diese Funktion auch ohne LAN-Verbindung anbieten.
[<=]

TIP1-A_2961 - Authentifizierung und MAC-Adressenabfrage
Wird die MAC-Adresse des eHealth-Kartenterminals nach [TIP1-A_2958] über eine lokale Terminalfunktion zur Anzeige gebracht, dann MUSS das eHealth-Kartenterminal eine Abfrage über eine lokale Terminalfunktion ohne Authentifikation bereitstellen.
[<=]

2.3.9.2 Aufbringen eines Prüfzeichens

TIP1-A_2962 - Spezifizierung gematik-Prüfzeichen
Das eHealth-Kartenterminal MUSS auf dem Gehäuse über ein gematik-Prüfzeichen verfügen, welches nicht unbeschadet ablösbar sein darf.
[<=]

TIP1-A_2964 - Anbringung gematik-Prüfzeichen
Der Hersteller des eHealth-Kartenterminals MUSS das gematik-Prüfzeichen an einer während der PIN-Eingabe für den Benutzer gut sichtbaren Stelle am eHealth-Kartenterminal aufbringen.
[<=]

TIP1-A_3107 - Optische Gestaltung des Prüfzeichens
Der Hersteller des eHealth-Kartenterminals MUSS sicherstellen, dass die optische Gestaltung des Prüfzeichens einer der beiden Varianten aus Abbildung [PIC_KT_0001] entspricht.
[<=]

TIP1-A_2963 - Prüfzeichen und inverse Form
Der Hersteller des eHealth-Kartenterminals KANN das Prüfzeichen gemäß [TIP1-A_3107] in inverser Form (Weiß auf schwarzem Untergrund) aufbringen.
[<=]

TIP1-A_3105 - Mindestgröße gematik Prüfzeichen
Der Hersteller des eHealth-Kartenterminal MUSS das gematik-Prüfzeichen auf das eHealth-Kartenterminal mit der Mindesthöhe 8 mm aufbringen.
[<=]

TIP1-A_3109 - EPS-Datei „gematik Prüfzeichen“
Der Hersteller des eHealth-Kartenterminals MUSS das in der EPS-Datei "gematik-Prüfzeichen" (PIC_KT_0001) vorgegebene Seitenverhältnis für das Prüfzeichen beibehalten.
[<=]

Die Berechtigung und Verpflichtung zur Nutzung des Prüfzeichens durch den Hersteller erfolgt mit der Zulassung der Geräte durch die gematik. Im Rahmen des Zulassungsantrags werden den Herstellern die beiden Versionen des gematik-Prüfzeichens im Encapsulated PostScript (EPS) Format zur Verfügung gestellt. Das Prüfzeichen bietet einen Wiedererkennungswert für zugelassene Kartenterminals, es sind keine Sicherheitsfunktionen damit verbunden.

Die Farbgebung des Prüfzeichens ist vierfarbig CMYK:

- für den Grün-Anteil: C40, M0, Y60, K0
- für den Rot-Anteil: C0, M100, Y100, K0
- für den Gelb-Anteil: C0 , M20, Y100, K0



Abbildung 3: PIC_KT_0001 – gematik-Prüfzeichen

2.3.10 Kommunikationsprotokolle

TIP1-A_3189 - Unterstützung IPv4
Das eHealth-Kartenterminal MUSS IPv4 unterstützen.
[<=]

TIP1-A_3190 - Unterstützung IPv6
Das eHealth-Kartenterminal SOLL in der Lage sein, IPv4 und IPv6 nur mittels eines Firmware Updates zu unterstützen.
[<=]

Nur bei eHealth-Kartenterminals, die auf bereits zugelassenen eHealth-BCS-Geräten basieren, kann eine Nichterfüllung der Anforderung akzeptiert werden.

TIP1-A_5656 - Unterstützung Auto-IP-Protokoll optional
Das eHealth-Kartenterminal KANN abweichend von den Regelungen in [SICCT#6.1.2] auf die Unterstützung des Auto-IP-Protokolls gemäß [RFC3927] verzichten.
[<=]

2.3.11 Firmware Update

TIP1-A_2965 - Sichere Updatemöglichkeit KT-Firmware
Das eHealth-Kartenterminal MUSS über eine sichere Update-Möglichkeit der KT-Firmware verfügen, welche es ermöglicht, alle Softwarebestandteile, ausgenommen ROM-Bereiche, zu aktualisieren.
[<=]

Hierunter ist sowohl der Wechsel auf eine neuere Firmware als auch ein Downgrade auf eine über das Konzept der Firmware-Gruppen (siehe Abschnitt 2.4.1.1) zugelassene Firmware zu verstehen.

TIP1-A_3188 - Erhaltung Konfigurationen nach Update
Das eHealth-Kartenterminal MUSS nach einem Firmware-Update sämtliche Konfigurationen, wie zum Beispiel Terminal-Name, IP-Adresse oder Pairing-Informationen, erhalten.
[<=]

Die sicherheitstechnischen Anforderungen an das Firmware-Update sind Kapitel 2.4.1.1 zu entnehmen.

Im Folgenden werden unter dem Begriff Update-Komponente jene Funktionalitäten im LAN zusammengefasst, welche das Firmware-Update entsprechend der Vorgaben dieser Spezifikation umsetzt, unabhängig davon, auf welchen Komponenten (Kartenterminal und/oder Drittsystem) diese umgesetzt wird.

TIP1-A_3152 - KT: Update-Komponente innerhalb des LAN
Hersteller des eHealth-Kartenterminals MÜSSEN eine Update-Komponente zur Verfügung stellen, über welche innerhalb des in der dezentralen Umgebung installierten LANs die Firmware des eHealth-Kartenterminals aktualisiert werden kann.
[<=]

TIP1-A_3153 - Update-Varianten für eHealth-Kartenterminals
Zur Umsetzung von [TIP1-A_3152] MUSS der Hersteller des eHealth-Kartenterminals mindestens eine der beiden folgenden Update-Varianten für eHealth-Kartenterminals umsetzen:
Push-Verfahren
Eine LAN-spezifische Update-Komponente wird auf einem Drittsystem innerhalb des LANs betrieben welche die Firmware-Updates auf den Kartenterminals einspielt. Das Verfahren zur Bereitstellung der Firmware-Updates auf einer LAN-spezifischen Update-Komponente ist herstellerspezifisch (z. B. organisatorische Prozesse).
Pull-Verfahren
eHealth-Kartenterminals beziehen Firmware-Updates selbstständig von einem Update-Server welcher auf einem Drittsystem innerhalb des LANs lokalisiert sein kann. Das Verfahren zur Bereitstellung der Firmware-Updates auf einer LAN-spezifischen Update-Komponente ist herstellerspezifisch (z. B. organisatorische Prozesse).
[<=]

Die Konfiguration der Update-Komponente ist ebenso wie deren Realisierung sowie die Details zum Mechanismus, mit dem ein Firmware-Update auf den Kartenterminals über das LAN eingespielt wird, herstellerspezifisch (beispielsweise kann das Firmware-Update über die SICCT-Schnittstelle eingespielt werden).

Zusätzlich zur herstellerspezifischen Update-Komponente unterstützt das Kartenterminal die Update-Funktionen der SICCT-Spezifikation, wodurch eine ansteuernde Komponente in die Lage versetzt wird, das Kartenterminal zu aktualisieren (z. B. der KSR-Dienst der Telematikinfrastruktur).

TIP1-A_6481 - Firmwarelieferung via P_KSRS_Upload Schnittstelle
Der Hersteller des eHealth-Kartenterminals MUSS jede zugelassene Firmware-Version umgehend als Update-Paket über die in [gemSpec_KSR] definierte Schnittstelle P_KSRS_Upload im Konfigurationsdienst (KSR) ablegen.
[<=]

2.3.12 Terminal Managementverfahren

TIP1-A_2966 - eHealth-Kartenterminal und direkte Managementschnittstelle
Ein eHealth-Kartenterminal MUSS über eine direkte Managementschnittstelle verfügen, welche zur Interaktion das Display sowie die Eingabeeinheit des Kartenterminals nutzt.
[<=]

TIP1-A_2967 - Aktivierung weiterer Managementschnittstellen
Das eHealth-Kartenterminal MUSS über die direkte Managementschnittstelle mindestens die Möglichkeit bieten, administrative SICCT-Kommandos gemäß [SICCT# 6.2.2.1] zu erlauben und zu verbieten sowie weitere vorhandene Managementschnittstellen (siehe

[TIP1-A_2970]) zu aktivieren und zu deaktivieren.
[<=]

TIP1-A_2968 - Aktivieren und Deaktivieren von weiteren Managementschnittstellen
Das eHealth-Kartenterminal MUSS die Aktivierung und Deaktivierung von Managementschnittstellen gemäß [TIP1-A_2970] ausschließlich über die direkte Managementschnittstelle ermöglichen.
[<=]

TIP1-A_2969 - Administration des eHealth-Kartenterminal
Das eHealth-Kartenterminal MUSS die Möglichkeit der Administration ausschließlich über die direkte Managementschnittstelle oder aktivierte Managementschnittstellen gemäß [TIP1-A_2970] erlauben.
[<=]

TIP1-A_2970 - Weitere Managementschnittstellen
Das eHealth-Kartenterminal KANN neben der direkten Managementschnittstelle über weitere Managementschnittstellen verfügen.
[<=]

TIP1-A_2971 - Über LAN-Netzwerk administrieren
Das eHealth-Kartenterminal KANN Schnittstellen anbieten, die es ermöglichen das eHealth-Kartenterminal über das LAN-Netzwerk zu administrieren.
[<=]

Diese Schnittstellen können sowohl vom Konnektor, von Administrationsprogrammen der Hersteller als auch über das Webinterface durch den Administrator bedient werden (siehe auch Kapitel 2.4.5). LAN-Schnittstellen zur Administrierung sind mittels TLS gesichert (siehe Kapitel 2.4.5.1).

TIP1-A_3263 - Dokumentation der Konfiguration
Der Hersteller des eHealth-Kartenterminals MUSS den Anwender bzw. den Administrator in geeigneter Form (z. B. in der Benutzerdokumentation) über alle für die Konfiguration notwendigen Parameter einschließlich nötiger Eigenschaften (z. B. Zweck, Wertebereich, Abhängigkeiten) informieren.
[<=]

Aus den Sicherheitsforderungen des PP kann es sich ergeben, dass einzelne Managementfunktionen als sicherheitsrelevant eingestuft werden und daher Interaktionen an der lokalen Managementschnittstelle des KTs erfordern. Näheres hierzu ergibt sich aus dem PP und ist herstellerspezifisch umzusetzen.

2.3.12.1 Anzeige des SICCT-Terminalnamens

TIP1-A_3144 - SICCT-Terminalname
Das eHealth-Kartenterminal MUSS den SICCT-Terminalnamen (siehe [SICCT#6.1.3.1]) des Kartenterminals über eine lokale Terminalfunktion auf dem Display zur Anzeige bringen.
[<=]

TIP1-A_3145 - Anzeige des SICCT-Terminalnamens
Das eHealth-Kartenterminal MUSS die Funktion zur Anzeige des SICCT-Terminalnamens immer zur Verfügung stellen, solange keine SICCT-Session am eHealth-Kartenterminal aktiv ist.
[<=]

TIP1-A_3146 - Abfrage SICCT-Terminalnamen
Das eHealth-Kartenterminal MUSS die lokale Terminalfunktion zur Anzeige des SICCT-Terminalnamens ohne Authentifikation anbieten.
[<=]

2.3.12.2 Produkttypversion und Selbstauskunft

Die Anforderungen bezüglich der Produkttypversion und Selbstauskunft sind in [gemSpec_OM] festgelegt. Hierüber hinaus gilt:

TIP1-A_3938 - Darstellung Selbstauskunft
Das eHealth-Kartenterminal MUSS die Rückgabe der Selbstauskunft dem Administrator über die direkte Managementschnittstelle ermöglichen.
[<=]

TIP1-A_3939 - Darstellung Firmware-Gruppen-Version
Das eHealth-Kartenterminal MUSS im Zuge der Selbstauskunft die aktuell installierte Firmware-Gruppen-Version darstellen.
[<=]

2.3.13 Mehrwertmodule

TIP1-A_3160 - Mehrwertmodule auf KT
Ein Hersteller KANN Mehrwertmodule (MWM) auf einem eHealth-Kartenterminal installieren, um z. B. zusätzliche Anwendungen in einem eHealth-Kartenterminal zu ermöglichen.
[<=]

Die gleichzeitige Verwendung von eHealth-Applikationen und herstellerspezifischen Mehrwertmodulen kann ein Sicherheitsrisiko darstellen.

Um die Sicherheit bei gleichzeitiger Verwendung von MWM und eHealth-Applikationen sicher zu stellen, ist der Nachweis der informationstechnischen Trennung von Mehrwertmodulen Bestandteil der Zulassung bzw. deren Evaluierung. Mehrwertmodule werden von der gematik nicht zugelassen.

TIP1-A_3036 - Mehrwertmodule: keine Störungen der eHealth-Anwendungen
Der Hersteller des eHealth-Kartenterminal MUSS sicherstellen, dass Mehrwertmodule keine Störungen der eHealth-Anwendungen verursachen und nicht auf Bereiche der eHealth-Anwendungen zugreifen, dies schließt auch eHealth-Anwendungen auf der eGK und dem HBA mit ein.
[<=]

TIP1-A_3161 - Mehrwertmodule KT de-/aktivierbar
Das eHealth-Kartenterminal SOLL dem Administrator die Möglichkeit bieten, die Mehrwertmodule zu aktivieren und zu deaktivieren, wobei der Mechanismus herstellerspezifisch ist.
[<=]

TIP1-A_3162 - Erkennbarkeit, ob Mehrwertmodul aktiv ist
Das eHealth-Kartenterminal MUSS jederzeit für den Benutzer klar ersichtlich anzeigen, ob aktuell ein eHealth-Dienst oder ein Mehrwertmodul des eHealth-Kartenterminals aktiv ist.
[<=]

TIP1-A_3261 - alleinige KT-Kontrolle über Anzeigemechanismus Diensttypaktivität
Das eHealth-Kartenterminal MUSS sicherstellen, dass der Mechanismus gemäß [TIP1-A_3162], mit dem angezeigt wird, welcher Diensttyp aktiv ist, unter der alleinigen Kontrolle des Kartenterminals liegt und es insbesondere nicht möglich ist, dass ein Mehrwertmodul diese Anzeige manipulieren kann.
[<=]

TIP1-A_3262 - SM-KT-Identität für Mehrwertmodule nutzbar
Das eHealth-Kartenterminal DARF den Zugriff eines Mehrwertmoduls auf die auf der SM-KT gespeicherte Identität NICHT unterbinden.
[<=]

2.3.14 Zugriffsanzeige

TIP1-A_2972 - Anzeige Kartenzugriffe
Das eHealth-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.

TIP1-A_2973 - Anzeige Zugriffe
Bei der Anzeige gemäß [TIP1-A_2972] MUSS das eHealth-Kartenterminal zumindest den Umstand anzeigen, dass auf eine Karte im eHealth-Kartenterminal zugegriffen wird und dies für die gesamte Dauer des Zugriffs.
[<=]

2.3.15 Desinfektion der Kartenterminals (informativ)

Hersteller seien darauf hingewiesen, dass eHealth-Kartenterminals auch in Einsatzumgebungen verwendet werden können, die einem erhöhten Übertragungsrisiko für Infektionen, z. B. durch häufigen Hand- und Hautkontakt, ausgesetzt sind. Die regelmäßige Desinfektion der eingesetzten Geräte beim Leistungserbringer, dazu gehören auch Kartenterminals, ist eine Maßnahme zur Verminderung des Übertragungsrisikos und zur Einhaltung entsprechender Vorgaben, z. B. denen des Arbeitsschutzgesetzes. Weiterführende Informationen sind unter anderem den folgenden Dokumenten zu entnehmen:

1. Anforderungen an die Hygiene bei der Reinigung und Desinfektion von Flächen des Robert-Koch-Institutes [RKI],
2. Technischen Regeln für biologische Arbeitsstoffe im Gesundheitswesen und in der Wohlfahrtspflege [TRBA 250],
3. Hygieneleitfaden des Deutschen Arbeitskreises für Hygiene in der Zahnmedizin [DAHZ].

2.3.16 Produktsicherheit (informativ)

Das Kartenterminal darf nur in den Verkehr gebracht werden, wenn Sicherheit und Gesundheit von Anwendern nicht gefährdet werden. Dazu muss der Anwender der

Produkte über alle Sicherheitsinformationen zum Produkt informiert werden. Auch muss der Kartenterminalhersteller den Lebenszyklus seines Produktes beobachten und bei bekannt gewordenen Mängeln die zuständige Behörde informieren und gegebenenfalls einen Rückruf einleiten. Das Kartenterminal muss den Anforderungen aus dem Gesetz über die Bereitstellung von Produkten auf dem Markt, kurz genannt Produktsicherheitsgesetz (ProdSG) entsprechen [PRODSG].

2.3.17 Physikalische Sicherheit-Klima

Als normaler Einsatzort wird für das eHealth-Kartenterminal ein Büroraum / ein Behandlungsraum angenommen.

TIP1-A_3930 - Physikalische Sicherheit-Klima
Das eHealth-Kartenterminal MUSS für den Einsatzort Büroraum bzw. Behandlungsraum die Anforderungen gemäß „Tab_KT_003 Anforderungen Klima" erfüllen.
[<=]

Tabelle 1: Tab_KT_003 Anforderungen Klima

Prüfung Klima
Trockene Wärme (Dry Heat) nach DIN EN 60068-2-2 Methode Bb wird für die Bedingungen als obere Lagertemperatur von 55°C und einer Beanspruchungsdauer von 16 h geprüft und die Funktionsfähigkeit MUSS bestätigt werden.
Kälte (Cold) nach DIN EN 60068-2-1 Methode Ab wird für die Bedingungen als untere Lagertemperatur von -10°C und einer Beanspruchungsdauer von 16 h geprüft und die Funktionsfähigkeit MUSS bestätigt werden.
Nach den beiden oben genannten Belastungen durch extreme Lagertemperaturen und der Nachbehandlungsdauer von 1 h MUSS die Funktionsfähigkeit des Kartenterminals gewährleistet sein, was durch Funktionsprüfungen nachzuweisen ist.
Die Funktionsfähigkeit im Betrieb MUSS bei einer oberen Temperatur von 40°C über eine Dauer von 2 h gewährleistet sein. Dies wird für das Kartenterminal durch Prüfung nach DIN EN 60068-2-2 Methode Bb bei gleichzeitigen Funktionsprüfungen nachgewiesen.

2.3.18 Physikalische Sicherheit-Vibration

Die durch Vibrationen und mechanische Schockbelastungen auftretenden Belastungen müssen vom Kartenterminal schadensfrei gemäß IEC 60068-2 Methode nach den folgenden Anforderungen absolviert, geprüft und nachgewiesen werden.

TIP1-A_3932 - Physikalische Sicherheit-Vibration
Das eHealth-Kartenterminal MUSS die Anforderungen gemäß „Tab_KT_004 Anforderungen Vibration“ erfüllen.
[<=]

Tabelle 2: Tab_KT_004 Anforderungen Vibration

Prüfung Vibration
Sinusförmige Schwingungstests (Vibration, sinusoidal) nach DIN EN 60068-2-6 Methode Fc in

drei senkrecht stehenden Achsen in einem Frequenzbereich von 2 Hz bis 200 Hz üblicherweise 1 h je Achse MÜSSEN erfolgreich nachgewiesen werden. Bis zu einer Frequenz von 9 Hz wird dabei mit einer konstanten Amplitude von 1,5 mm belastet, darüber bis zur oberen Frequenz wird mit einer konstanten Beschleunigung von 5 m/s^2 (0,5 g) belastet.
Es MÜSSEN mechanische Schockprüfungen (Shock) nach DIN EN 60068-2-27 Methode Ea in drei senkrecht stehenden Achsen (sechs Richtungen) erfolgreich nachgewiesen werden. Es wird dabei für jede Achse mit 3 positiven und 3 negativen Schocks mit 150 m/s^2 (15 g) Amplitude und einer Dauer von 11 ms belastet.
Dauerschocktests (Bump) nach DIN EN 60068-2-29 Methode Eb in drei senkrecht stehenden Achsen mit halbsinusförmigen Schocks MÜSSEN erfolgreich nachgewiesen werden. Es wird dabei für jede Achse mit 1000 positiven und 1000 negativen Schocks mit 100 m/s^2 (10 g) Amplitude und einer Dauer von 16 ms belastet.

2.3.19 Benutzerfreundlichkeit und weitere Kennwort-/PIN-Eingaben

In den relevanten Dokumenten zum eHealth-Kartenterminal sind verschiedene Credentials detailliert spezifiziert. Dabei handelt es sich z.B. um das Direktkennwort zur Sicherung der direkten Managementschnittstelle, Administratorkennwörter zur Sicherung weiterer Managementschnittstellen, das Passwort zur Sicherung der CT ADMIN Session ([SICCT]) sowie optional Kennwörter zur Authentifizierung von weiteren Nutzern.

Weitere herstellerspezifische Credentials (z.B. zum Schutz des Shared Secrets durch Verschlüsselung), die sich durch die Verwendung geeigneter Hardware-Sicherungsmaßnahmen vermeiden lassen, dürfen unter dem Aspekt der Benutzerfreundlichkeit nicht notwendig sein. Jede weitere Abfrage von Credentials, insbesondere wenn sie nicht zum Schutz von Managementschnittstellen bei Administration sondern auch im Regelbetrieb notwendig ist, verringert die Benutzerfreundlichkeit und damit die Akzeptanz des Geräts erheblich.

TIP1-A_6541 - Benutzerfreundlichkeit und weitere Kennwort-/PIN-Eingaben
Das eHealth-Kartenterminal SOLL neben den in dieser Spezifikation ([gemSpec_KT]), in [SICCT] und in [BSI-CC-PP-0032] definierten NICHT weitere Kennwort-, Passwort- bzw. PIN-Eingaben (auch als credentials bezeichnet) außerhalb des PIN-Handlings von Karten erforderlich machen.
[<=]

Nur bei eHealth-Kartenterminals, die auf bereits zugelassenen eHealth-BCS-Geräten basieren und bei denen die Umstellung vom eHealth-BCS-Spezifikationsstand auf den eHealth-Spezifikationsstand per Firmware Upgrade (Firmware Update) erfolgt, kann eine Nichterfüllung der Anforderung [TIP1-A_6541] akzeptiert werden.

2.4 Spezielle sicherheitstechnische Anforderungen

Basissicherheitsanforderungen sind im Kapitel 8 der SICCT-Spezifikation [SICCT] beschrieben. Des Weiteren sind die Anforderungen aus der Technischen Richtlinie TR-03120 [TR-03120] sowie dem Anhang zur TR-03120 [TR-03120-Anhang] (Versiegelung) verpflichtend umzusetzen.

2.4.1 Firmware Update

Das eHealth-Kartenterminal muss über eine gesicherte Update-Möglichkeit der KT-Firmware verfügen (siehe Kapitel 2.3.11).

TIP1-A_3182 - Erkennung von Übertragungsfehlern und nicht authentischen Übertragungen während eines Firmware-Updates
Der zur Erkennung von Übertragungsfehlern und nicht authentischen Übertragungen während eines Firmware Updates des eHealth-Kartenterminals notwendige Sicherheitsanker MUSS in einem über die äußeren Schnittstellen auslesegeschützten Bereich des eHealth-Kartenterminals liegen.
[<=]

TIP1-A_3185 - Ablage des Sicherheitsankers in einem schreibgeschützten Bereich des KT
Das eHealth-Kartenterminal MUSS den für die authentische Übertragung und zur Erkennung von Übertragungsfehlern eines Firmware Updates genutzten Sicherheitsanker in einem schreibgeschützten Bereich des Terminals ablegen, welcher nur im Rahmen eines administrativen Vorgangs ausgetauscht werden können darf.
[<=]

TIP1-A_3183 - selbständige Übertragungsfehlererkennung bei KT-Firmware-Updates
Der vom eHealth-Kartenterminal genutzte Mechanismus zur Übertragung von Firmware Updates SOLL in der Lage sein, Übertragungsfehler selbstständig zu erkennen.
[<=]

Für das Verwaltungsverfahren gelten mindestens die Anforderungen, die in der Sicherheitsevaluierung und dem zugehörigen Protection Profile sowie den Sicherheitszielen zu Grunde gelegt werden.

TIP1-A_2976 - Prüfung Integrität/Authentizität einer neuen Firmware
Das eHealth-Kartenterminal MUSS sicherstellen, dass nur nach erfolgreicher Prüfung der Integrität und Authentizität der zu installierenden Firmware ein Einspielen möglich ist.
[<=]

TIP1-A_2977 - Fehlerhafte oder nicht authentische Übertragung abweisen
Das eHealth-Kartenterminal MUSS den Firmware-Download bei einer fehlerhaften oder nicht authentischen Übertragung abweisen.
[<=]

TIP1-A_3245 - Keine Veränderung bei fehlerhafter oder nicht authentischer Übertragung
Das eHealth-Kartenterminal DARF eine Veränderung an der aktuellen, zertifizierten und installierten Firmware-Version bei einer fehlerhaften oder nicht authentischen Übertragung einer anderen Firmware-Version NICHT vornehmen.
[<=]

TIP1-A_2978 - Übernahme als aktive Firmware
Das eHealth-Kartenterminal MUSS sicherstellen, dass eine Firmware nur dann als aktive Firmware übernommen wird, nachdem sie vollständig und korrekt in den Speicher übernommen wurde.
[<=]

Die Notwendigkeit des Wechsels auf eine Vorversion der installierten Firmware kann sich u. a. aus den folgenden Gründen ergeben:

- aus Betriebsgründen, z. B. zur kurzfristigen Behebung eines aufgetretenen Fehlverhaltens.
- im Rahmen der Migration, um Rollback-Szenarien bei der Einführung neuer Releases zu ermöglichen.

Dieser Wechsel der Firmware kann z. B. durch ein Firmware Downgrade (ein Wechsel auf eine Firmware mit kleinerer Versionsnummer) realisiert werden. Aus Sicherheitsgründen sind solche Firmware Downgrades allerdings nur eingeschränkt und unter Berücksichtigung der im „Konzept der Firmwaregruppen“ beschriebenen Anforderungen (Kapitel 2.4.1.1) erlaubt. Die Art der Versionierung ist unter der Einhaltung der Vorgaben aus [gemSpec_OM] herstellerspezifisch.

2.4.1.1 Konzept der Firmware-Gruppen

Das Konzept der Firmwaregruppen wird in [gemSpec_OM] beschrieben. Weitere Anforderungen in diesem Zusammenhang ergeben sich aus [gemSpec_KSR]. Über die dortigen Anforderungen hinaus gilt:

TIP1-A_3170 - Ausführen eines zulässigen Downgrades
Der Hersteller des eHealth-Kartenterminals MUSS dafür sorgen, dass der Administrator vor dem Ausführen eines zulässigen Downgrades über die herstellerspezifische Update-Komponente auf die möglichen Konsequenzen hingewiesen wird - z. B. im Rahmen der Benutzerdokumentation - und die Möglichkeit erhält, den Downgrade-Prozess noch abzubrechen.
[<=]

2.4.2 Anzeige des vertrauenswürdigen Zustands

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 (siehe Kapitel 3.11) Daher braucht der vertrauenswürdige Zustand nicht zwingend angezeigt werden.

TIP1-A_3038 - Vertrauenswürdiger Zustand
Der Hersteller des eHealth-Kartenterminals MUSS entweder den vertrauenswürdigen Zustand am Gerät anzeigen oder, wenn der vertrauenswürdige Zustand nicht am Gerät angezeigt wird, in der Benutzerdokumentation allgemeinverständlich beschreiben, dass das eHealth-Kartenterminal sicherheitsrelevante SICCT- bzw. EHEALTH-Befehle ausschließlich in einem vertrauenswürdigen Modus ausführt.
[<=]

Der vertrauenswürdige Zustand bleibt auch während der Ausführung von Mehrwertmodulen erhalten (siehe Kapitel 2.3.13).

2.4.3 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.

TIP1-A_2979 - Aktivierung und Erkennbarkeit sicherer PIN-Modus
Das eHealth-Kartenterminal MUSS bei jeder PIN-Eingabe (direkt oder im Remote-PIN-Verfahren) den sicheren PIN-Modus gemäß [SICCT#7.6] aktivieren und den sicheren Pin-Modus dem Benutzer anzeigen.
[<=]

Da sich eine Remote-PIN Eingabe auch um eine PIN-Eingabe handelt, befindet sich das eHealth-Kartenterminal auch bei der Remote-PIN Eingabe in diesem sicheren PIN-Modus. Eine separate Anzeige, dass es sich um eine Remote-PIN-Eingabe handelt, ist nicht erforderlich.

2.4.4 Sicherheitsanforderungen LAN-gekoppelter Terminals

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

- 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, bei der es sich um eine Kombination von zwei Verfahren handelt, z. B. aus Wissen (PIN) und Besitz (Karte)).

TIP1-A_3415 - Sicherung der Netzwerkkommunikation
Das eHealth-Kartenterminal MUSS für die Sicherung der Netzwerkkommunikation die TLS-Versionen gemäß [gemSpec_Krypt] implementieren.
[<=]

Für die Sicherung der hierfür notwendigen Netzwerkkommunikation sind~~ist~~ für alle Kartenterminals die in [gemSpec_Krypt] genannten Verfahren ~~TLS 1.1 (Transport Layer Security) gemäß [RFC4346] [gemSpec_Krypt#GS-A_4386]~~ als einheitliche~~s~~ auf Zertifikaten basierende~~s~~ Verfahren vorgegeben. ~~Um die Zukunftsfähigkeit zu gewährleisten, soll zusätzlich auch TLS 1.2 gemäß [RFC5246] unterstützt werden [gemSpec_Krypt#GS-A_4385].~~ 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) gehörige geheime Schlüssel (PrK.SMKT.AUT) ist in einem manipulationsgeschützten Speicher (SM-KT) verwahrt, der einen unbefugten Zugriff auf das Schlüsselmaterial verhindert.

2.4.5 Terminal Managementverfahren

TIP1-A_2980 - Managementschnittstellen zur Administrierung
Das eHealth-Kartenterminal MUSS sicherstellen, dass das Abfragen und Ändern der sicherheitskritischen Konfiguration an Managementschnittstellen erst nach erfolgreicher Authentisierung an diesen möglich ist.
[<=]

TIP1-A_2981 - Rolle Administrator
Im Rahmen der Administration MUSS das eHealth-Kartenterminal mindestens die Rolle Administrator umsetzen.
[<=]

TIP1-A_3412 - Nähere Beschreibung Rolle Administrator
Das eHealth-Kartenterminal MUSS sicherstellen, dass ausschließlich die Rolle Administrator Einstellungen zur Benutzerverwaltung, Netzwerkkonfiguration, den Terminal- und Slot-Namen ändern, Pairing-Information löschen, sofern vorhanden eine PUK gemäß [TIP1-A_3421] ändern, Firmware-Updates einspielen, Mehrwertmodule aktivieren und deaktivieren (sofern vorhanden) sowie Komponentenzertifikate für Konnektoren verwalten kann.
[<=]

TIP1-A_2982 - Rolle Benutzer und Administration
Das eHealth-Kartenterminal MUSS sicherstellen, falls die Rolle Benutzer für die Administration des Kartenterminals umgesetzt ist, dass der Benutzer nur berechtigt ist, sich die aktuellen Einstellungen anzeigen zu lassen und sein eigenes Kennwort zu ändern.
[<=]

TIP1-A_2983 - Übertragung medizinischer und personenbezogener Daten
Das eHealth-Kartenterminal DARF medizinische und personenbezogene Daten NICHT über Managementschnittstellen übertragen.
[<=]

TIP1-A_2984 - Anzeige medizinischer und personenbezogener Daten
Das eHealth-Kartenterminal DARF medizinische und personenbezogene Daten NICHT über Managementschnittstellen anzeigen.
[<=]

2.4.5.1 Sicherung der administrativen TLS-Verbindung

Nach [TIP1-A_3415] sind Netzwerkverbindungen grundsätzlich mit den in [gemSpec_Krypt] genannten Verfahren zu sichern. ~~Die Verbindung zu den Netzwerk-basierten Managementschnittstellen ist immer mit TLS 1.1 gemäß [RFC4346] zu sichern [gemSpec_Krypt#GS-A_4386]. Um die Zukunftsfähigkeit zu gewährleisten sollen sie auch mittels TLS 1.2 gemäß [RFC5246] gesichert werden können [gemSpec_Krypt#GS-A_4385].~~

TIP1-A_3246 - Port der netzwerkbasierten Managementschnittstellen
Das eHealth-Kartenterminal DARF den SICCT-Port NICHT als Port einer netzwerkbasierten Managementschnittstelle des eHealth-Kartenterminals, die keine SICCT-Session nutzt, für Schnittstellen gemäß [TIP1-A_2971] nutzen.
[<=]

TIP1-A_3231-01 - TLS-Verbindung: einseitige Authentisierung
Das eHealth-Kartenterminal MUSS als Authentisierungsverfahren für administrative TLS-Verbindungen ~~gemäß [GS-A_4386]~~ mindestens einseitige Authentisierung einsetzen.
[<=]

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

TIP1-A_3232 - Sicherung administrativer TLS-Verbindung
Das eHealth-Kartenterminal KANN ergänzend zu [TIP1-A_3231] zur Sicherung der administrativen TLS-Verbindung gegenseitige Authentisierung einsetzen.
[<=]

TIP1-A_3233 - Einseitige Authentisierung während des Aufbaus der administrativen TLS-Verbindung
Das eHealth-Kartenterminal (Server) MUSS sich im Fall einer einseitigen Authentisierung für den Aufbau der administrativen TLS-Verbindung gemäß [TIP1-A_3231] gegenüber dem Client (z. B. Webbrowser) authentisieren.
[<=]

Als Bestandteil der Authentisierung ist auch ein eventuell sicheres Einbringen eines Zertifikates in den Client anzusehen.

TIP1-A_3947 - Dokumentation Einbringung Serverzertifikat
Ist für die Nutzung einer Managementverbindung ein sicheres Einbringen eines Zertifikates in einen Client notwendig, dann MUSS der Hersteller des eHealth-Kartenterminals das Verfahren der notwendigen Authentizitätsprüfung im Rahmen des Einbringens des Zertifikates in den Client in seiner Benutzerdokumentation beschreiben.
[<=]

Das Kartenterminal hat für die administrative TLS-Verbindung die in [gemSpec_Krypt#5.9] angeführten Algorithmen, wie in [gemSpec_Krypt#A_17089] und [gemSpec_Krypt#A_17090] definiert, zu unterstützen.

TIP1-A_2985 - Schlüsselmaterial des SM-KT
Das eHealth-Kartenterminal MUSS für den Aufbau des administrativen TLS-Kanals das Schlüsselmaterial des SM-KT (ID.SMKT.AUT) verwenden, sofern ein SM-KT vorhanden ist.
[<=]

TIP1-A_2986 - Kein SM-KT vorhanden
Das eHealth-Kartenterminal KANN Schlüsselmaterial sowie ein zugehöriges Zertifikat für den Aufbau der administrativen TLS-Verbindung zur Verfügung stellen (z. B. in der Firmware), falls kein SM-KT vorhanden ist.
[<=]

TIP1-A_3129 - TLS-Verbindungsaufbau: notwendiges kryptographisches Material
Falls das eHealth-Kartenterminal das für den TLS-Verbindungsaufbau notwendige kryptographische Material nicht zur Verfügung stellt und kein SM-KT vorhanden ist, so MUSS das eHealth-Kartenterminal sicherstellen, dass vorhandene netzwerkbasierte Managementschnittstellen deaktiviert sind.
[<=]

TIP1-A_3260 - Netzwerkbasierten Managementschnittstellen
Das eHealth-Kartenterminal MUSS die netzwerkbasierten Managementschnittstellen deaktivieren, wenn kein SM-KT vorhanden ist und das eHealth-Kartenterminal selbst über keinen für den Verbindungsaufbau notwendigen Zufallszahlengenerator verfügt.
[<=]

TIP1-A_3234 - Private Schlüssel zur Sicherung des administrativen TLS-Kanals
Das eHealth-Kartenterminal MUSS private Schlüssel zur Sicherung des administrativen TLS-Kanals vor Veränderung und Auslesen geschützt speichern.
[<=]

TIP1-A_3235 - Öffentliche Schlüssel und Zertifikate zur Sicherung des administrativen TLS-Kanals
Das eHealth-Kartenterminal MUSS öffentliche Schlüssel zur Sicherung des administrativen TLS-Kanals vor Veränderung geschützt speichern.
[<=]

Es sei darauf hingewiesen, dass die Nutzung desselben Zertifikats für alle Kartenterminals einer Baureihe mit einem Risiko behaftet ist, da der zugehörige private Schlüssel auf allen Kartenterminals einer Baureihe verteilt ist. Details zu den Vorgaben an die Zertifikate sind Bestandteil der Sicherheitsevaluierung.

2.4.5.2 Anforderungen an Kennwörter zur Sicherung der Managementschnittstelle

Im Folgenden werden die Anforderungen an die Kennwörter zur Sicherung der Managementschnittstellen aufgeführt. Das Administratorkennwort, welches lokal direkt an der Tastatur des Kartenterminals (im Folgenden direkte Managementschnittstelle, siehe auch Kapitel 2.3.12) eingegeben wird, wird als Direktkennwort bezeichnet.

TIP1-A_2987 - Aktivierung direkte Managementschnittstelle
Das eHealth-Kartenterminal MUSS nach Setzen des Direktkennwortes die direkte Managementschnittstelle aktivieren.
[<=]

TIP1-A_3236 - Kennworteingabe bei der Aktivierung einer weiteren Managementschnittstelle
Das eHealth-Kartenterminal KANN bei Aktivierung einer weiteren Managementschnittstelle für diese ein neues Administratorkennwort an der direkten Managementschnittstelle abfragen.
[<=]

TIP1-A_2988 - Administratorkennwort eingegeben an der direkten Managementschnittstelle
Das eHealth-Kartenterminal KANN das an der direkten Managementschnittstelle für eine weitere Managementschnittstelle eingegebene Administratorkennwort für alle anderen verfügbaren Managementschnittstellen (ausgenommen Direktkennwort) als deren jeweiliges Administratorkennwort übernehmen.
[<=]

TIP1-A_2989 - Separates Setzen der Kennwörter
Das eHealth-Kartenterminal MUSS sicherstellen, dass für jede Managementschnittstelle separat ein Kennwort gesetzt werden kann.
[<=]

TIP1-A_2990 - Fehlerzähler bei falscher Kennworteingabe
Das eHealth-Kartenterminal MUSS für jede Managementschnittstelle einen eigenen Fehlerzähler falscher Kennworteingaben vorhalten.
[<=]

TIP1-A_2991 - Fehlerzähler: Veränderung über Schnittstelle
Das eHealth-Kartenterminal DARF es NICHT ermöglichen, Fehlerzähler falscher Kennworteingaben über externe Schnittstellen zu verringern.
[<=]

TIP1-A_2992 - Fehlerzähler: Abfrage
Das eHealth-Kartenterminal KANN Fehlerzähler falscher Kennworteingaben von einem Benutzer abfragbar machen.
[<=]

TIP1-A_2993 - Geschütze Speicherung der Kennwörter
Das eHealth-Kartenterminal MUSS die Kennwörter der Managementschnittstellen geschützt speichern, sodass sie nicht ausgelesen oder unberechtigt verändert werden können.
[<=]

TIP1-A_2994 - Sperrzeiten für direkte Managementschnittstelle bei Falscheingabe
Das eHealth-Kartenterminal MUSS den Zugang des jeweiligen Benutzers oder Administrators zur direkten Managementschnittstelle ab der dritten aufeinander folgenden ungültigen Kennworteingabe an dieser Schnittstelle sperren, wobei die Dauer der Sperrzeit von der Anzahl aufeinander folgender Fehlversuche abhängig ist und gilt:

- Bei 3-6 Fehlversuchen beträgt die Sperrzeit 1 Minute.
- Bei 7-10 Fehlversuchen beträgt die Sperrzeit 10 Minuten.
- Bei 11-20 Fehlversuchen beträgt die Sperrzeit 1 Stunde.
- Ab 21 Fehlversuchen beträgt die Sperrzeit 1 Tag.

[<=]

TIP1-A_2995 - Fehlerzähler: spannungsloser Zustand
Das eHealth-Kartenterminal MUSS Fehlerzähler falscher Kennworteingaben im spannungslosen Zustand erhalten.
[<=]

TIP1-A_2996 - Fehlerzähler: Speicherung verstrichener Sperrzeit im spannungslosem Zustand
Das eHealth-Kartenterminal KANN die bereits verstrichene Sperrzeit während einer Direktkennworteingabe oder einer Kennworteingabe an einer weiteren Managementschnittstelle im spannungslosen Zustand erhalten und den Zugang zur jeweils betroffenen Schnittstelle nach Neustart nur für die verbleibende Zeit sperren.
[<=]

TIP1-A_2997 - Fehlerzähler: Neustart Sperrzeit nach spannungslosem Zustand
Das eHealth-Kartenterminal MUSS, falls es die bereits verstrichene Wartezeit nicht im spannungslosen Zustand erhält, die Sperrzeit nach einem Neustart, unabhängig von der bereits verstrichenen Sperrzeit, wieder der dem Fehlerzähler entsprechenden Mindestsperrzeit setzen.
[<=]

TIP1-A_2998 - Sperrung weiterer Managementschnittstellen bei Falscheingabe
Das eHealth-Kartenterminal MUSS, mit Ausnahme der direkten Managementschnittstelle, den Zugang des jeweiligen Benutzers oder Administrators zu einer Managementschnittstelle ab der dritten aufeinander folgenden ungültigen Kennworteingabe an dieser Schnittstelle sperren. Die Dauer der Sperrzeit ist von der Anzahl aufeinander folgender Fehlversuche abhängig und muss gemäß den diesbezüglichen Regelungen in [TIP1-A_2994] umgesetzt werden.
[<=]

TIP1-A_2999 - Sperrung weiterer Managementschnittstellen für alle Benutzer bei Falscheingabe
Das eHealth-Kartenterminal KANN die Managementschnittstelle ab der dritten aufeinander folgenden ungültigen Kennworteingabe eines Benutzers an dieser Managementschnittstelle, mit Ausnahme der direkten Managementschnittstelle, auch für alle weiteren Benutzer sperren. Die Dauer der Sperrzeit ist von der Anzahl aufeinander folgender Fehlversuche abhängig und muss gemäß den diesbezüglichen Regelungen in [TIP1-A_2994] umgesetzt werden.
[<=]

TIP1-A_3416 - Prüfung Stellen des Kennwortes
Das eHealth-Kartenterminal MUSS die Prüfung eines Kennwortes gegen das vollständige Kennwort durchführen (und nicht nur einen Kennwortausschnitt).
[<=]

Für alle Kennwörter zur Sicherung einer Managementschnittstelle gelten folgende Anforderungen.

TIP1-A_3000 - Mindestanforderungen Kennwort
Das eHealth-Kartenterminal MUSS sicherstellen, dass Kennwörter zur Sicherung der Managementschnittelle des eHealth-Kartenterminals mindestens acht Zeichen lang sind und mindestens aus Ziffern (‚0' bis ‚9') bestehen.
[<=]

TIP1-A_3001 - Zeichen für Kennwort
Das eHealth-Kartenterminal KANN Kennwörter zur Sicherung der Managementschnittelle des eHealth-Kartenterminals unterstützen, die aus einer Mischung aus Ziffern, Buchstaben und Sonderzeichen bestehen.
[<=]

TIP1-A_3002 - Beschränkung für Kennwortauswahl
Das eHealth-Kartenterminal DARF eine zur Rollen-Authentisierung verwendete Benutzer-ID als Teilzeichenkette NICHT als Bestandteil eines Kennwortes unterstützen.
[<=]

TIP1-A_3003 - Kennwörter und programmierbare Funktionstasten
Das eHealth-Kartenterminal DARF die Speicherung von Kennwörtern auf programmierbaren Funktionstasten NICHT unterstützen.
[<=]

TIP1-A_3004 - Kennwort und Klartextanzeige
Das eHealth-Kartenterminal DARF ein Kennwort bei dessen Eingabe NICHT im Klartext anzeigen.
[<=]

Zusätzliche, nicht normative Informationen zur Handhabung von Kennwörtern sind im vom BSI herausgegebenen Maßnahmenkatalog Organisation (M 2) Abschnitt 11 „Regelungen des Passwortgebrauchs“ [BSI-M2.11] beschrieben.

2.4.5.3 Anforderungen an die PUK für die Durchführung des Werksresets

Im Folgenden werden die Anforderungen an die PUK zur Sicherung des Werksresets aufgeführt, wenn dieser Mechanismus vom Hersteller umgesetzt ist.

TIP1-A_3422 - PUK-Eingabe bei Inbetriebnahme
Das eHealth-Kartenterminal MUSS im Fall der Umsetzung des Werksresets durch [TIP1-A_3421] bei der Inbetriebnahme den Administrator nach Eingabe des Direktkennwortes auffordern, eine PUK einzugeben.
[<=]

TIP1-A_3423 - Fehlerzähler PUK
Das eHealth-Kartenterminal MUSS im Fall der Umsetzung des Werksresets durch [TIP1-A_3421] einen eigenen Fehlerzähler für die PUK implementieren.
[<=]

Weiterhin müssen für die Sicherung des Werksresets durch ein PUK-Verfahren die folgenden Anforderungen aus Kap. 2.4.5.2 umgesetzt werden:

- einen Fehlerzähler für die PUK Eingabe implementieren und diesen im spannungslosen Zustand erhalten (siehe [TIP1-A_2995]).
- diese ab der dritten aufeinander folgenden ungültigen Eingabe der PUK sperren, wobei die Dauer der Sperrzeit von der Anzahl aufeinander folgender Fehlversuche abhängig ist (siehe [TIP1-A_2994]).
- sicherstellen, dass die PUK mindestens acht Zeichen lang ist und mindestens aus Ziffern (‚0' bis ‚9') besteht (siehe [TIP1-A_3000]). Die PUK kann auch aus einer Mischung aus Ziffern, Buchstaben und Sonderzeichen bestehen (siehe [TIP1-A_3001]) und darf eine zur Rollen-Authentisierung verwendete Benutzer-ID als Teilzeichenkette nicht enthalten (siehe [TIP1-A_3002]).
- sicherstellen, dass die PUK nicht auf programmierbaren Funktionstasten gespeichert werden kann (siehe [TIP1-A_3003]).
- sicherstellen, dass die PUK bei der Eingabe nicht im Klartext angezeigt wird (siehe [TIP1-A_3004]).
- sicherstellen, dass die PUK vollständig (und nicht nur ein Ausschnitt) geprüft wird (siehe [TIP1-A_3416]).

TIP1-A_5083 - Anforderungen PUK
Das eHealth-Kartenterminal MUSS im Fall der Umsetzung des Werksresets durch [TIP1-A_3421] die Anforderungen [TIP1-A_2994], [TIP1-A_2995], [TIP1-A_3000], [TIP1-A_3001], [TIP1-A_3002], [TIP1-A_3003], [TIP1-A_3004], sowie [TIP1-A_3416] entsprechend für die PUK umsetzen.
[<=]

Zusätzliche, nicht normative Informationen zur Handhabung von Kennwörtern sind im vom BSI herausgegebenen Maßnahmenkatalog Organisation (M 2) Abschnitt 11 „Regelungen des Passwortgebrauchs" [BSI-M2.11] beschrieben.

2.4.6 Übergreifende Sicherheitsanforderungen

Die übergreifenden Sicherheitsanforderungen resultieren aus dem Schutzbedarf der nachfolgenden Sicherheitsobjekte:

- Signatur-PIN und Qualifizierte Signatur des Leistungserbringers bzw. eines Mitarbeiters einer Organisation des Gesundheitswesens
- PINs

- Session Key oder Objektschlüssel

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.

TIP1-A_3239 - Persistente Speicherung im Kartenterminal
Das eHealth-Kartenterminal DARF Daten aus der Telematikinfrastruktur (TI) NICHT persistent speichern, außer (und dieses ist die einzige Ausnahme) Konfigurationsdaten zwischen Konnektor und Kartenterminal (inkl. Shared Secret für das Pairing).
[<=]

Hierunter fällt auch ein eventuelles Logging.

2.4.7 Protection Profile (Schutzprofil)

Das Protection Profile für Kartenterminals [BSI-CC-PP-0032] legt die Mindestanforderungen im Sinne von Sicherheitszielen für ein eHealth-Kartenterminal fest und beschreibt Funktionalitätsklassen. Das Protection Profile dient als Basis zur Durchführung einer Evaluierung im Rahmen der Zertifizierung nach Common Criteria des umfassenden Produkts. Die Anforderungen aus dem Protection Profile sind umzusetzen.

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

2.4.7.1 Umgebungsanforderungen für Kartenterminals

Die Anforderungen an die Einsatzumgebung der Kartenterminals werden im Kapitel der Annahmen des Schutzprofils [BSI-CC-PP-0032] des BSI festgelegt und müssen vom Hersteller bei der Evaluierung berücksichtigt werden.

2.4.8 Zufallszahlen und Schlüssel

Ein Zufallsgenerator erzeugt Zufallszahlen und Schlüssel im Rahmen bestimmter Kryptoverfahren, wie z. B. Challenge-Response-Authentifizierung bei TLS.

TIP1-A_3005 - Zufallszahlen und Einmalschlüsseln
Das eHealth-Kartenterminal MUSS das Erstellen von Zufallszahlen und Einmalschlüsseln unterstützen.
[<=]

Die Länge der angeforderten Zufallszahlen bzw. Einmalschlüssel und die Qualität des Generators ist vom jeweiligen Einsatzzweck abhängig. Die entsprechenden Regelungen sind [gemSpec_Krypt#GS-A_4367] zu entnehmen.

TIP1-A_3039 - Quelle für Zufallszahlen Zufallszahlengenerator des SM-KT
Das eHealth-Kartenterminal KANN als Quelle für Zufallszahlen den Zufallszahlengenerator des SM-KT verwenden, welcher die Anforderungen an Qualität und Güte der Zufallszahlen nach [gemSpec_Krypt#GS-A_4367] erfüllt.
[<=]

Da das SM-KT erst in das Kartenterminal eingebracht werden muss, steht der Zufallszahlengenerator des SM-KT nicht immer zur Verfügung.

TIP1-A_3040 - Erzeugung von Zufallszahlen ohne vorhandenes SM-KT
Das eHealth-Kartenterminal KANN zur Erzeugung von Zufallszahlen ohne vorhandenes SM-KT mindestens einen rein in Software umsetzbaren Zufallszahlengenerator zur Verfügung stellen.
[<=]

TIP1-A_3241 - Abweichung von [gemSpec_Krypt#2.2]
Das eHealth-Kartenterminal KANN den gemäß [TIP1-A_3040] umgesetzten Zufallszahlengenerator mit einer geringeren Qualität und die erzeugten Zufallszahlen mit einer geringeren Güte implementieren, als in [gemSpec_Krypt#2.2] gefordert.
[<=]

Dieser Zufallszahlengenerator kann, selbst wenn er die Anforderungen an Qualität und Güte aus [gemSpec_Krypt#2.2] nicht erfüllt, zum Aufbau von nicht SICCT-spezifischen TLS-Verbindungen verwendet werden.

TIP1-A_3242 - Nicht SICCT-spezifische TLS-Verbindungen und [gemSpec_Krypt#2.2]
Das eHealth-Kartenterminal KANN, wenn kein SM-KT im eHealth-Kartenterminal vorhanden ist, den Zufallszahlengenerator des Kartenterminals gemäß [TIP1-A_3040] zum Aufbau von nicht SICCT-spezifischen TLS-Verbindungen verwenden.
[<=]

TIP1-A_3041 - Zufallszahlengenerator geringerer Güte
Das eHealth-Kartenterminal DARF einen Zufallszahlengenerator geringerer Güte gemäß [TIP1-A_3241] NICHT zum Aufbau von SICCT-spezifischen TLS-Verbindungen nutzen.
[<=]

Es liegt in der Verantwortung der Hersteller im Rahmen der Sicherheitsevaluierung nachzuweisen, dass durch den Einsatz des Zufallszahlengenerators des Kartenterminals kein Schaden entstehen kann.

2.5 Festlegungen zu Kartenterminalidentität und Schlüsselmanagement

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.

TIP1-A_3227 - Umsetzung der KT-Identität
Das eHealth-Kartenterminal MUSS zur Umsetzung der KT-Identität die SM-KT-Identität (ID.SMKT.AUT), bestehend aus einem Schlüsselpaar (PuK.SMKT.AUT, PrK.SMKT.AUT) mit zugehörigem X.509-Zertifikat (C.SMKT.AUT), nutzen, welche auf einer Smartcard bereitgestellt wird und die an das SM-KT gestellten Sicherheitsanforderungen erfüllt.
[<=]

Die KT-Identität besteht aus der Kombination

- der Anforderung [TIP1-A_3227] und
- einem nachfolgend ausgehandelten gemeinsamen Geheimnis (ShS.KT.AUT) zwischen Kartenterminal und Konnektor (im Folgenden als Shared Secret bezeichnet, siehe auch 2.5.2).

Die SMKT-Identität wird u. a. zur Identifikation und Schlüsselaushandlung zwischen der Signaturanwendungskomponente (des Konnektors) und dem Kartenterminal genutzt. In einer LAN-Umgebung wird die „alleinige Kontrolle“ schwer darstellbar und kann nur über entsprechend sichere Identitäten und authentifizierte Verbindungen zu Kartenterminals wiederhergestellt werden.

Das SM-KT muss den privaten Schlüssel (PrK.SMKT.AUT) gegen ein Auslesen bzw. Vervielfachen sichern. Intention dieses Schutzmechanismus ist es nicht, die Integrität der Kartenterminal-Firmware gegen Angriffe zu schützen. Das SM-KT ist auf einer gSMC-KT in ID-000 Form aufgebracht.

Der Hersteller des eHealth-Kartenterminals ist der Herausgeber der Gerätekarte gSMC-KT.

TIP1-A_6717 - gSMC-KT Verantwortung durch den Hersteller
Der Hersteller des eHealth-Kartenterminals MUSS die Rolle des Kartenherausgebers für Gerätekarten gSMC-KT zu eHealth-Kartenterminals dieses Herstellers einnehmen. Der Hersteller des eHealth-Kartenterminals KANN die von ihm verantwortete Personalisierung der gSMC-KT und die vertrauenswürdige Auslieferung an einen Leistungserbringer bzw. an eine Organisation des Gesundheitswesens durch einen von ihm zu beauftragenden Dienstleister in seinem Namen vornehmen lassen.
[<=]

TIP1-A_7016 - Prüfung der personalisierten gSMC-KT
Der Hersteller des eHealth-Kartenterminals MUSS sich von der korrekten Personalisierung der herausgegebenen gSMC-KT überzeugen.
[<=]

TIP1-A_6718 - Bezugsquellen gSMC-KT
Der Hersteller des eHealth-Kartenterminals MUSS im Handbuch des eHealth-Kartenterminals die Bezugsquelle für eine Gerätekarte gSMC-KT aufführen.
[<=]

TIP1-A_6719 - Prüfung von Authentizität und Integrität der gSMC-KT
Der Hersteller MUSS es dem Administrator des eHealth-Kartenterminals ermöglichen, die Authentizität und Integrität der gSMC-KT vor dem Pairing mit dem eHealth-Kartenterminal prüfen zu können. Der Hersteller MUSS im Handbuch des eHealth-Kartenterminals diese Prüfmöglichkeiten beschreiben und den Administrator auf die Prüfung der Integrität und Authentizität vor dem Pairing hinweisen.
[<=]

Dem Administrator soll damit eine Handreichung gegeben werden, welche Prüfungen nach Empfang einer gSMC-KT und vor deren Verwendung durchzuführen sind. Der Administrator sollte beispielsweise nur eine gSMC-KT verwenden, die auch tatsächlich bestellt wurde und beim Empfang prüfen, ob die Verpackung und die Karte unversehrt sind und ob der Absender auch dem erwarteten Absender entspricht. Hierzu ist es notwendig, dass der Hersteller entsprechende Angaben zu Bezugsquellen und möglichen Versandadressen macht. Diese Angaben können im Handbuch und/oder auf der Webseite des Herstellers verfügbar gemacht werden. Dies muss für den Administrator aus dem Handbuch ersichtlich sein. Vor der Verwendung der gSMC-KT sollte der Administrator auch eine optische Prüfung der gSMC-KT vornehmen, um eventuelle Manipulationen der Karte auf dem Transportweg zu erkennen. Darin kann ihn beispielweise das Handbuch unterstützen, in welchem optische Merkmale der gSMC-KT beschrieben sind oder diese abgebildet ist. Diese im Handbuch zu beschreibenden grundlegenden Prüfungen, die ein Administrator vor Verwendung einer empfangenen

gSMC-KT durchführen muss, sind hier nur allgemein und beispielhaft aufgeführt und müssen an die herstellerspezifischen Abläufe angepasst werden.

TIP1-A_6720 - Verwendung zugelassener Gerätekarten gSMC-KT
Der Hersteller MUSS ausschließlich von der gematik zugelassene Gerätekarten gSMC-KT herausgeben.
[<=]

TIP1-A_3180 - Zugriff auf DF.KT
Nutzt das Kartenterminal das DF.KT einer vom Konnektor adressierbaren gSMC-KT als SM-KT, dann MUSS das Kartenterminal ausschließlich über den Basiskanal 0 auf dieses DF.KT zugreifen.
[<=]

TIP1-A_3181 - Priorisierung DF.KT Zugriff
Nutzt das Kartenterminal das SM-KT gemäß [TIP1-A_3180], dann MUSS das eHealth-Kartenterminal die im Rahmen der Nutzung der Kartenterminalidentität von ihm selbst gesendeten Karten-Kommandos priorisieren und die Bearbeitung von eventuell vorhandenen Client-SICCT-Kommandos unterbrechen und deren Bearbeitung erst nach Beendigung der internen Kommandosequenz fortsetzen.
[<=]

Die Reaktion auf die Unterbrechung obliegt dem Hersteller. Kommandos können sowohl mit einer Fehlermeldung beantwortet als auch intern gequeued werden.

Das SM-KT wird durch Stecken in einen entsprechenden ID-000 Slot oder mittels Adapter in einen Slot anderen Formats in das Kartenterminal eingebracht. Nach den Vorgaben des Protection Profiles [BSI-CC-PP-0032] und der Technischen Richtlinie [TR-03120] sowie dessen Anhangs ist die Karte so in das Terminal einzubringen, dass Manipulation verhindert bzw. erkannt werden können. Hierfür ist somit eine der in [TIP1-A_3059] geforderten Kontaktiereinheiten zu nutzen.

TIP1-A_3192 - Anforderungen an Slotsiegel
Wird die Sicherung des Steckplatzes zur Karte, welcher das SM-KT enthält, gemäß [TIP1-A_3059] mit einem Siegel (sog. Slotsiegel, das nicht dem Gehäusesiegel entspricht) gesichert, MUSS der Hersteller den Anhang der technischen Richtlinie [TR-03120] für die Anforderungen an diese Siegel berücksichtigen und dem Nutzer diese Siegel zur Verfügung stellen (mindestens vier Slotsiegel im Rahmen der Auslieferung des Gerätes).
[<=]

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 2.5.2 beschrieben.

TIP1-A_3229 - Schutz vor Auslesen des Shared Secrets
Das eHealth-Kartenterminal MUSS das Shared Secret vor Auslesen geschützt speichern, wobei die Anforderungen aus [BSI-CC-PP-0032] zum Schutz vor Auslesen des Shared Secret umzusetzen sind.
[<=]

TIP1-A_3043 - Speicherung Shared Secret
Das eHealth-Kartenterminal DARF das Shared Secret NICHT auf dem SM-KT speichern.
[<=]

Eine Verschlüsselung des Shared Secrets ist nicht erforderlich.

TIP1-A_3112 - Entnahme des SM-KT
Das eHealth-Kartenterminal MUSS sicherstellen, dass bei einer Entnahme des SM-KT, während eine TLS-Verbindung besteht, die unter Verwendung des entnommenen SM-KT aufgebaut wurde, keine zusätzliche Bedrohung zum Fall einer Entnahme des SM-KT ohne eine solche bestehende TLS-Verbindung entsteht.
[<=]

Beispielsweise kann dies umgesetzt werden, indem das Kartenterminal bei Entnahme des SM-KT eventuell aktive TLS-Verbindungen, die die korrespondierende SMKT-Identität zum Betreiben des TLS-Kanals nutzen, aktiv beendet. 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.
- passive Maßnahmen, bei denen das SM-KT nur in einem Zustand des Geräts gesteckt oder entfernt werden kann, während dem keine TLS-Verbindung unter Verwendung des SM-KT möglich ist (z. B. Zugang zum SM-KT Kartenschacht nur nach Entfernen der LAN- und Powerkabel möglich)

2.5.1 Anforderungen an die Kartenterminalidentität

2.5.1.1 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 und der verwendeten PKI sind in [gemSpec_PKI] beschrieben. Die zugehörigen Object Identifier (OID) sind im Dokument [gemSpec_OID] festgelegt. Das Zertifikat wird im DER-Format auf der Karte gespeichert.

Grundsätzlich müssen die Schlüssel der SMKT-Identitäten in einem sicheren Schlüsselspeicher hinterlegt sein. Dieser Schlüsselspeicher wird SM-KT genannt. Das 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 eine Benutzerverifikation nicht erforderlich sein darf,
3. dem Kartenterminal einen Zufallszahlengenerator mit einer Entropie von mind. 100 Bit bieten,
4. den öffentlichen Schlüssel frei auslesen lassen.

Das SM-KT muss den Fingerprint des enthaltenen X.509-Zertifikats für die SMKT-Identitäten lesbar aufgedruckt haben oder der Fingerprint muss dem SM-KT zuordenbar auf einer gesonderten Liste mitgeliefert werden.

Das Zertifikat der SMKT-Identität auf dem 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 hat.

Eine PIN-Freischaltung dieser Chipkarte darf nicht notwendig sein.

Genaue Festlegungen zur Filestruktur und den Zugriffsrechten des SM-KT werden in [gSMC-KT] getroffen.

2.5.1.2 Bedeutung für das Kartenterminal

TIP1-A_3044 - Erstellung des Authentifizierungstokens
Das eHealth-Kartenterminal MUSS für seine Authentifikation bei der TLS-Verbindung zum Konnektor auf das SM-KT für die Erstellung des Authentifizierungstokens zurückgreifen.
[<=]

Die TLS-Verbindung auf Seiten des Kartenterminals terminiert aber nicht im SM-KT, sondern im Terminal selbst.

2.5.1.3 Produktion und Auslieferung

Produktion, Auslieferung und Inbetriebnahme müssen aufeinander abgestimmt sein und sicherstellen, dass nur integere Kartenterminals eine gültige KT-Identität erhalten und beim Leistungserbringer bzw. bei Organisationen des Gesundheitswesens zum Einsatz kommen

TIP1-A_3413 - Prüfung Authentizität und Integrität bei Inbetriebnahme
Der Hersteller des eHealth-Kartenterminals MUSS in der Benutzerdokumentation den Administrator darauf hinweisen, dass der Administrator die Integrität des Terminals vor der Inbetriebnahme überprüfen muss.
[<=]

2.5.2 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. Um zu verhindern, dass der auf dem SM-KT gespeicherte Teil der kryptographischen Identität des Kartenterminals aus einem Kartenterminal entfernt und unbefugt in einem anderen Terminal genutzt werden kann, schafft das Pairing eine logische Verbindung von Kartenterminal und SM-KT. Die Gesamtheit aus logischer Verbindung sowie kryptographischer Identität des SM-KT bildet die Kartenterminalidentiät.

TIP1-A_3045 - Pairing-Information
Das eHealth-Kartenterminal MUSS die Pairing-Information in Pairing-Blöcken verwalten.
[<=]

TIP1-A_3046 - Pairing-Block
Das eHealth-Kartenterminal MUSS je Pairing-Block mindestens drei öffentliche Schlüssel von Konnektorzertifikaten und einen Shared Secret aufnehmen können.
[<=]

Alle öffentlichen Schlüssel, die in demselben Pairing-Block gespeichert sind, korrespondieren zu dem ebenfalls in diesem Pairing-Block gespeicherten Shared Secret.

TIP1-A_3047 - Zugriff auf Shared Secrets
Das eHealth-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 Einsatzumgebung des Kartenterminals ab. In jedem Fall darf das Shared Secret nicht auf dem SM-KT im Terminal gespeichert werden (siehe [TIP1-A_3043]).

TIP1-A_3048 - Shared Secrets und Klartextanzeige
Das eHealth-Kartenterminal DARF Shared Secrets NICHT im Klartext zur Anzeige bringen.
[<=]

TIP1-A_3049 - Löschung Pairing-Blöcke
Das eHealth-Kartenterminal MUSS über eine Möglichkeit verfügen, zum Zwecke der Administration ganze Pairing-Blöcke zu löschen.
[<=]

TIP1-A_3050 - Löschung öffentliche Schlüssel
Das eHealth-Kartenterminal MUSS über eine Möglichkeit verfügen, zum Zwecke der Administration gezielt einzelne öffentliche Schlüssel aus einem Pairing-Block zu löschen.
[<=]

TIP1-A_3051 - Löschen von Pairing-Informationen
Das eHealth-Kartenterminal MUSS sicherstellen, dass das Löschen von Pairing-Informationen nur über die Rolle Administrator möglich ist.
[<=]

TIP1-A_3006 - Mindestanzahl Pairing-Block
Das eHealth-Kartenterminal MUSS mindestens einen Pairing-Block speichern können.
[<=]

TIP1-A_3007 - Empfohlene Anzahl Pairing-Blöcke
Das eHealth-Kartenterminal SOLL mindestens zwei Pairing-Blöcke speichern können.
[<=]

TIP1-A_3067 - Anzahl Konnektorverbindungen
Das eHealth-Kartenterminal DARF NICHT gleichzeitig Verbindungen zu mehr als einem Konnektor unterhalten.
[<=]

TIP1-A_3943 - Pairing zwischen Konnektor und eHealth-Kartenterminal
Das Pairing zwischen Konnektor und eHealth-Kartenterminal MUSS sicher erfolgen.
[<=]

TIP1-A_3243 - Initiales Pairing
Der Hersteller des eHealth-Kartenterminals MUSS den Administrator, der das Pairing des Kartenterminals durchführt, in einer geeigneten Form informieren (z.B. über die Benutzerdokumentation), dass der Administrator während des Prozesses sicherstellen muss, dass das Kartenterminal während des Initialen Pairings in seiner organisatorischen Hoheit steht, sodass keine unauthorisierten Dritten während des Pairings Zugang zum Kartenterminal oder zum Konnektor erlangen können.
[<=]

Im Rahmen des Pairings existieren drei Abläufe:

- Initiales Pairing: dient der logischen Verbindung von Kartenterminal und SM-KT aus Sicht des Konnektors mittels Shared Secret
- Überprüfung der Pairing-Informationen: Der Konnektor prüft nach Aufbau der TLS-Verbindung als zweiten Schritt der Authentisierung, ob das Kartenterminal im Besitz des Shared Secrets ist.
- Wartungs-Pairing: Bekanntmachung eines neuen Konnektorzertifikates am Kartenterminal unter Nutzung eines bekannten Shared Secret

Diese Abläufe und die Verfahrensweise bzgl. der Pairing-Informationen bei der Außerbetriebnahme eines Kartenterminals werden im Folgenden beschrieben.

2.5.2.1 Initiales Pairing

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

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

Schritt 1: Einbringen eines eHealth-Kartenterminals im dezentralen Netzwerk:

Im ersten Schritt des Pairing-Verfahrens bringt der Administrator das eHealth-Kartenterminal ins das in der dezentralen Umgebung installierte LAN ein, wobei die Konfiguration des eHealth-Kartenterminals gemäß [#6.1.1] erfolgt. Um die Verwaltung zu vereinfachen, soll der SICCT-Terminalname auch bei Nichtnutzung von DHCP bei der Inbetriebnahme des Kartenterminals gesetzt werden. Dieser wird im Dienstbeschreibungspaket übertragen und kann in der Kartenterminalverwaltung des Konnektors im Sinne eines Friendly Name verwendet werden.

Der Administrator prüft die Unversehrtheit und Authentizität des eHealth-Kartenterminals, notiert sich dessen eindeutiges Identifikationsmerkmal (z. B. die MAC-Adresse oder den SICCT-Terminalnamen; die Eindeutigkeit eines SICCT-Terminalnamens während des initialen Pairings wird durch den Konnektor sichergestellt) zusammen mit dem Fingerprint eines noch nicht zugeordneten SM-KT zur späteren Überprüfung und bringt dieses SM-KT anschließend in das eHealth-Kartenterminal ein.

Nachdem der Administrator ein oder mehrere eHealth-Kartenterminals derart im dezentralen Netz 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 findet die logische Verbindung zwischen einem Kartenterminal und SM-KT statt. Der Gesamtablauf ist im Überblick in Abbildung „Pic_KT_0007 Initiales Pairing Schritt 2“ dargestellt.

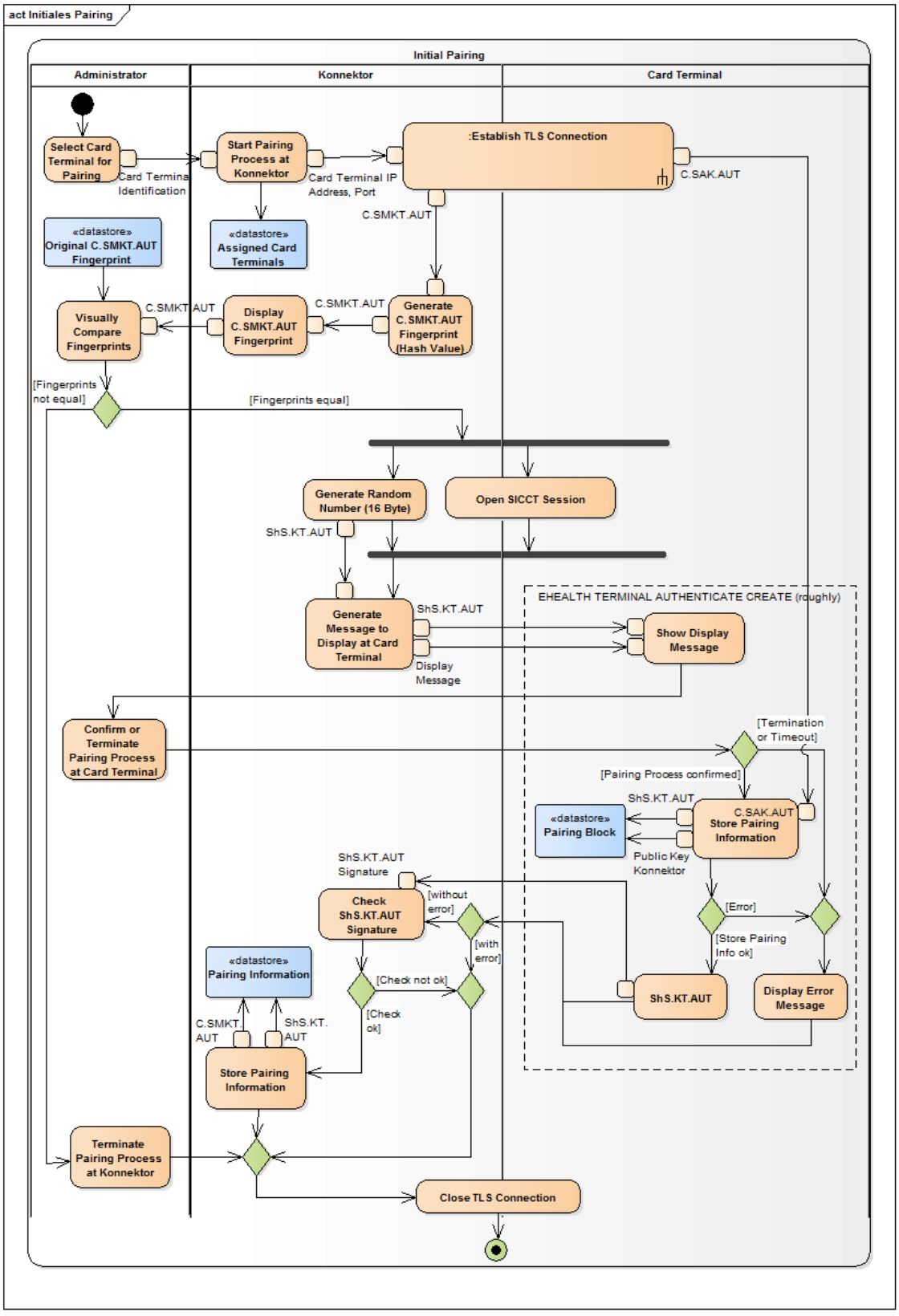


Abbildung 4: Pic_KT_0007 Initiales Pairing Schritt 2

Der Administrator wählt an der Kartenterminalverwaltung des Konnektors anhand des eindeutigen Identifikationsmerkmals des Kartenterminals (z. B. dessen SICCT-Terminalnamen oder MAC-Adresse) ein eHealth-Kartenterminal aus, welches mit dem Konnektor gepairt werden soll.

Daraufhin baut der Konnektor eine TLS-Verbindung (siehe Kapitel 3.11) zum ausgewählten eHealth-Kartenterminal auf. Während dieses Verbindungsaufbaus erhält der Konnektor das X.509-Zertifikat des 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 (ShS.KT.AUT) bezeichnet) und sendet die Kennung zusammen mit einer Display-Meldung (die Display-Meldung wird im Konnektor festgelegt) mit Hilfe des Pairing-Befehls EHEALTH TERMINAL AUTHENTICATE (siehe Kapitel 3.7.2) über die TLS-Verbindung an das Kartenterminal. Das Kartenterminal zeigt die Display-Meldung an und wartet auf eine Bestätigung mittels Druck auf die Bestätigungs-Taste am PIN Pad. Wird die Bestätigungs-Taste nicht innerhalb einer herstellerspezifischen Zeitspanne, die maximal 10 Minuten betragen darf, gedrückt oder wird der Abbruch-Button gedrückt, so bricht das Kartenterminal den Vorgang mit einer entsprechenden Fehlermeldung ab. Die Überprüfung des Kartenterminals vor Abschluss des Pairings durch den Administrator dient dazu, die Integrität und Authentizität des eHealth-Kartenterminals zum Zeitpunkt der Inbetriebnahme sicherzustellen.

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

Zum Abschluss des Prozesses sendet das Kartenterminal die mittels des 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 dem eindeutigen Identifikationsmerkmal des Kartenterminals. Die Inbetriebnahme ist damit abgeschlossen.

2.5.2.2 Überprüfung der Pairing-Information 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 Pairing-Information 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. 3.7.2) an das Kartenterminal. Mit dem Kommando

wird an das Terminal ein mindestens 16 Byte großes/r Zufallsdatum/-wert übertragen. Das Kartenterminal hängt an das Zufallsdatum das korrespondierende Shared Secret aus den Pairing-Informationen, und errechnet dann von dem kompletten Array den SHA-256-Hash-Wert. Diesen Hash-Wert schickt das Kartenterminal als Response zurück an den Konnektor.

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

2.5.2.3 Pairing-Informationen bei Außerbetriebnahme

TIP1-A_3244 - Außerbetriebnahme eines eHealth-Kartenterminals
Der Hersteller des eHealth-Kartenterminals MUSS den Anwender bzw. den Administrator in geeigneter Form (z. B. in der Benutzerdokumentation) informieren, dass bei einer Außerbetriebnahme des eHealth-Kartenterminals alle Pairing-Informationen am eHealth-Kartenterminal gelöscht werden müssen.
[<=]

2.5.2.4 Wartungs-Pairing

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 (im Gegensatz zum initialen Pairing muss der Administrator beim Wartungs-Pairing nicht sicherstellen, dass sich alle Kartenterminals in seiner organisatorischen Hoheit befinden) 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 Pairing-Information durchführen. Der Mechanismus zum Übertragen von Pairing-Informationen zwischen zwei Konnektoren ist in [gemSpec_Kon] beschrieben.

Der Gesamtablauf des Wartungs-Pairings ist im folgenden Sequenzdiagramm informativ dargestellt. Die zugehörigen Kommandos und technischen Abläufe im Kartenterminal sind im Kapitel 3.7.2 definiert.

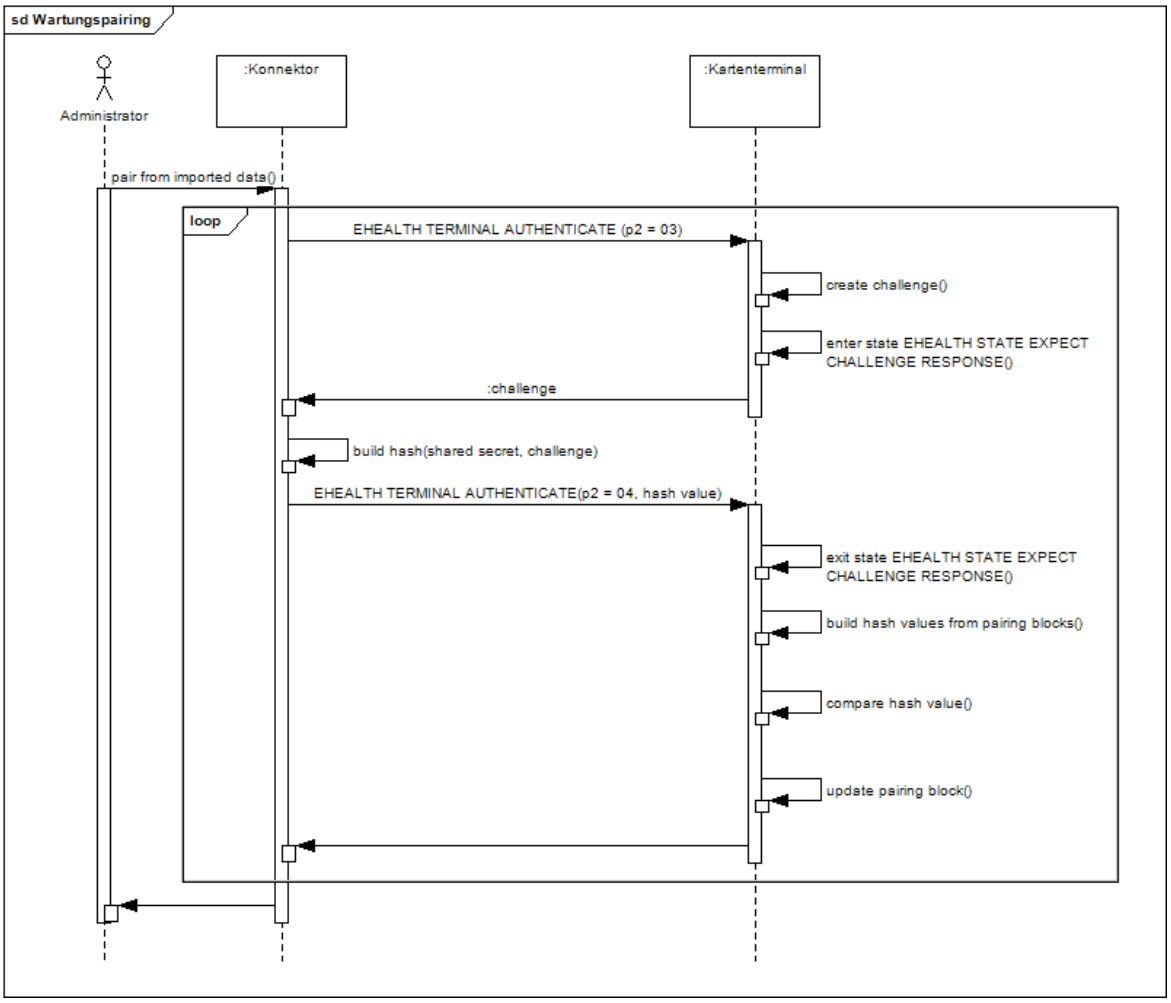


Abbildung 5: Pic_KT_0008 Wartungs-Pairing

Das Bekanntmachen eines neuen Konnektors unter Verwendung bereits bestehender Pairing-Information läuft in zwei 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-Hash-Wert. Diesen Hash-Wert 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 Pairing-Block ebenfalls den Hash-Wert aus Challenge und jeweiligem Shared Secret und vergleicht alle generierten Hash-Werte mit der Response des Konnektors. Falls das Kartenterminal die Response erfolgreich validieren und eindeutig einem Pairing-Block zuordnen kann, trägt das Kartenterminal den öffentlichen Schlüssel in den korrespondierenden Pairing-Block ein. Falls kein Platz für einen weiteren öffentlichen Schlüssel im korrespondierenden Pairing-Block vorhanden ist, überschreibt das Kartenterminal den ältesten öffentlichen Schlüssel des Pairing-Blocks.

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 (siehe Kapitel 3.7.2.2). 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.

3 Spezielle technische Anforderungen

3.1 Abgeleitete mechanische Anforderungen

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

3.1.1 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 [gSMC-KT].

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

TIP1-A_3926 - Karten-Kompatibilität
Das eHealth-Kartenterminal MUSS zu den in Tabelle „Tab_KT_005 Karten-Kompatibilität“ aufgeführten Karten kompatibel sein.
[<=]

Tabelle 3: Tab_KT_005 Karten-Kompatibilität

Karte	Referenz
KVK	[KVK]
eGK	[eGK]
HBA	[HBA]
gSMC-KT	[gSMC-KT]
SMC-B	[SMC-B]
ZOD Karten	[ZOD]
HBA-qSig-Karten	[HBA-qSig]

3.1.2 Kontaktiereinheiten

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

Allgemein gilt für das eHealth-Kartenterminal:

TIP1-A_3927 - Kontaktschonende Kontaktiereinheiten
Das eHealth-Kartenterminal MUSS kontaktschonende Kontaktiereinheiten verwenden.
[<=]

TIP1-A_3008 - Unterstützung Kartenkontakte
Das eHealth-Kartenterminal SOLL die Kartenkontakte C4, C6 und C8 NICHT unterstützen.
[<=]

TIP1-A_3009 - Elektrischer Anschluss Kartenkontakte
Das eHealth-Kartenterminal SOLL die Kartenkontakte C4, C6 und C8 NICHT elektrisch anschließen.
[<=]

TIP1-A_3929 - Landende Kontakte
Der Hersteller des eHealth-Kartenterminals SOLL Kontaktiereinheiten mit landenden Kontakten als kontaktschonende Kontaktiereinheiten gemäß [TIP1-A_3927] verwenden.
[<=]

TIP1-A_3130 - Kartenkontakte und Umschalten in andere Betriebsmodi
Das eHealth-Kartenterminal DARF, falls die Kartenkontakte C4, C6 und C8 für spezielle Betriebsmodi wie ISO7816-12 erforderlich sind, diese NICHT vor dem Umschalten in einen solchen Modus aktivieren.
[<=]

TIP1-A_3138 - Kartenkontakte und Umschalten Betriebsmodi
Das eHealth-Kartenterminal MUSS, falls die Kartenkontakte C4, C6 und C8 für spezielle Betriebsmodi wie ISO7816-12 erforderlich sind, diese initial, vor dem Umschalten in einen solchen Modus, potentialfrei setzen.
[<=]

3.1.2.1 ID-1 Kartenkontaktierungen

TIP1-A_3944 - Einführung oder Entnahme der Chipkarte
Das eHealth-Kartenterminal MUSS sicherstellen, dass die Entnahme oder Einführung der Chipkarte nicht zu einer Beschädigung der Bedruckung bzw. der Funktionalität der Karte durch die Kontaktiereinheit führt.
[<=]

TIP1-A_3010 - „Card-In“-Schalter
Das eHealth-Kartenterminal DARF den "Card-In"-Schalter (d. h. der Schalter zur Kartenpräsenzerkennung) NICHT vor Kontaktierung der Kontaktflächen und Erreichen des Kontakt-Enddrucks schalten.
[<=]

TIP1-A_3011 - Anpressdruck der Kontakte
Die Kontaktiereinheit des eHealth-Kartenterminals MUSS einen Anpressdruck der Kontakte der Kontaktiereinheit auf die Kontaktflächen der Karte von 0.2-0.6N haben.
[<=]

TIP1-A_3247 - Statusmeldung der Chipkarte
Das eHealth-Kartenterminal MUSS in der Lage sein, über ein Signal oder einen Status einer Applikation zu melden, wann sich die Chipkarte korrekt in der Kontaktiereinheit befindet und wann diese mit Strom versorgt ist und wenn diese entnommen wird.
[<=]

TIP1-A_3052 - Funktionsfähigkeit der Karte bei Notentnahme
Das eHealth-Kartenterminal MUSS, falls es mit einem Entnahmeschutz ausgestattet ist, in Ergänzung des Abschnitts 4.1.2 der SICCT-Spezifikation [SICCT] sicherstellen, dass eine gesteckte Karte auch nach einer Notentnahme noch funktionsfähig ist und keine mechanischen Beschädigungen durch die Entnahme aufweist.
[<=]

TIP1-A_3053 - Beschriftung/Bedruckung bei Notentnahme
Das eHealth-Kartenterminal MUSS eine Notentnahme einer Karte ohne Risiken für die Karte, auch der Bedruckung bzw. Beschriftung, sicherstellen.
[<=]

TIP1-A_3054 - Hilfsmittel Notentnahme
Das eHealth-Kartenterminal MUSS eine Notentnahme mit gebräuchlichen Werkzeugen bzw. Hilfsmitteln ermöglichen.
[<=]

Hier können als Hilfsmittel z. B. Büroklammern angesehen werden.

TIP1-A_3248 - Notentnahme vor Ort
Das eHealth-Kartenterminal MUSS eine Notentnahme einer Karte vor Ort ermöglichen.
[<=]

TIP1-A_3055 - Bauform eHealth-Kartenterminal
Das eHealth-Kartenterminal MUSS eine Bauform haben, die eine versehentliche Bedienung der Notentnahme einer Karte verhindert.
[<=]

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.

TIP1-A_3056 - Notentnahme bei Stromausfall
Das eHealth-Kartenterminal MUSS eine Notentnahme einer Karte ermöglichen, wenn die Stromversorgung des Kartenterminals ausgefallen ist.
[<=]

TIP1-A_3057 - Benutzerdokumentation für Notentnahme
Der Hersteller des eHealth-Kartenterminals MUSS die notwendige Handhabung des Terminals zur Durchführung der Notentnahme einer Karte in der Benutzerdokumentation des eHealth-Kartenterminals beschreiben.
[<=]

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

3.1.2.2 ID-000-Kartenkontaktierungen

TIP1-A_3249 - Zugriff auf die Plug-In-Karte
Das eHealth-Kartenterminal KANN den Zugriff auf die Plug-In-Karte(n) ohne Beschränkung des Zugangs zum Zwecke des Diebstahlschutzes ermöglichen, sofern die Anforderung [TIP1-A_3059] bereits erfüllt worden ist.
[<=]

Sofern native ID-000-Kontaktierungen vorhanden sind, gilt Anforderung [TIP1-A_3249] und es ist kein Card-In-Kontakt erforderlich.

3.1.3 Bauformen

TIP1-A_3058 - Unterstützung kontaktbehaftete Chipkarten
Das eHealth-Kartenterminal MUSS mindestens eine Kontaktiereinheit zur Aufnahme von Chipkarten im Format ID-1 haben.
[<=]

Die Bauform mit einem einzelnen ID-1-Slot eignet sich 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.

TIP1-A_3059 - eHealth-Kartenterminal und Kontaktiereinheiten
Das eHealth-Kartenterminal MUSS zusätzlich zu den ID-1-Kontaktiereinheiten mindestens zwei Kontaktiereinheiten bereitstellen, sodass zwei ID-000-Module gesichert im Kartenterminal steckbar sind.
[<=]

Durch die gesicherte Aufnahme wird die Möglichkeit der Erkennung von Manipulationen der Karte gegeben. Die Art der Sicherung ist herstellerspezifisch.

TIP1-A_3061 - Format Kontaktiereinheiten
Das eHealth-Kartenterminal KANN das Format der für die Aufnahmen von ID-000 Modulen bestimmten Kontaktiereinheiten herstellerspezifisch umsetzen, da das ID-000 Modul auch mittels eines Adapters gesteckt werden kann.
[<=]

3.2 Abgeleitete elektrische Anforderungen

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

3.2.1 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 von 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.

3.2.2 Reset-Verhalten und ATR-Bearbeitung

TIP1-A_3062 - Kommunikationsverhalten des Kartenterminals
Das eHealth-Kartenterminal MUSS, in Ergänzung zu den in Abschnitt 4.2.2 der SICCT-Spezifikation [SICCT] genannten Anforderungen an das Kommunikationsverhalten des Kartenterminals, die folgenden Mindestanforderungen umsetzen:

- Parameter Fn 372 und 512

- Parameter Dn bei 372 1, 2, 4, 12
- Parameter Dn bei 512 1, 2, 4, 8, 16, 32

[<=]

TIP1-A_3147 - Übertragungsparameter PPS1
Das eHealth-Kartenterminal SOLL im Rahmen des PPS-Verfahrens zur Aushandlung der Übertragungsrate zur Karte für den Übertragungsparameter PPS1 den Wert ‚97' unterstützen.
[<=]

Nur bei eHealth-Kartenterminals, die auf bereits zugelassenen eHealth-BCS-Geräten basieren, kann eine Nichterfüllung der Anforderung akzeptiert werden.

TIP1-A_3148 - TA1 Byte
Das eHealth-Kartenterminal SOLL, falls dem eHealth-Kartenterminal im TA1 Byte des ATR einer Karte der Wert ‚97' (entspricht Fn = 512 und Dn = 64) angezeigt wird, diesen Wert im Rahmen des PPS-Verfahrens in PPS1 verwenden.
[<=]

TIP1-A_3149 - PPS-Verfahren und Wert ‚97'
Das eHealth-Kartenterminal MUSS, falls es den Wert ‚97' im Rahmen des PPS-Verfahrens für PPS1 nicht unterstützt, für PPS1 einen Wert aus der Menge {´92´, ´93´, ´94´, ´95´, ´96´} verwenden.
[<=]

TIP1-A_3150 - Zusammenarbeit mit einer Karte die im TA1 Byte des ATR der Wert ‚97' zurückliefert
Das eHealth-Kartenterminal DARF die Zusammenarbeit mit einer Karte die im TA1 Byte des ATR den Wert ‚97' zurückliefert NICHT ablehnen.
[<=]

3.3 Transport von Zeichen

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

3.4 Chipkartenprotokolle

Die Protokolle sind nach den Vorgaben der jeweiligen internationalen Normen und der SICCT-Spezifikation zu implementieren. Es müssen im Rahmen der Chipkartenkommunikation alle Protokollfehler spezifikationskonform behandelt werden.

TIP1-A_3117 - Protokollfehler spezifikationskonform behandeln
Das eHealth-Kartenterminal SOLL dafür sorgen, dass bei unspezifizierten Fehlersituationen im Rahmen der Chipkartenkommunikation innerhalb eines Kontextes, dieses keine Auswirkung auf andere Kontexte hat.

[<=]

TIP1-A_3250 - Deadlock während Kartenkommunikation
Das eHealth-Kartenterminal MUSS das Auftreten eines Deadlocks während der Kartenkommunikation verhindern.
[<=]

Das Erkennen und Verhindern von Deadlocks während der Kartenkommunikation ist im hohen Maße von der herstellerspezifischen Implementierung der Firmware abhängig. Von einem Deadlock ist beispielsweise auszugehen, wenn Kommando-Sequenzen, die nur im Block ausgeführt werden dürfen (z. B. im Zusammenhang mit einer Autorisierung), von Kommandos auf einem anderen logischen Kanal unterbrochen werden und die begonnene Sequenz nicht abgeschlossen werden kann.

TIP1-A_3063 - Synchrone und asynchrone Übertragungsprotokolle
Das eHealth-Kartenterminal MUSS nachfolgend aufgeführte synchrone und asynchrone Übertragungsprotokolle zu den entsprechenden Chipkarten unterstützen.
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, z. B. als Token zum Auslösen der Komfortsignatur, durch das eHealth-Kartenterminal ist erlaubt.

Sollten kontaktlose Karten unterstützt werden, muss die Implementierung der Protokolle gemäß der SICCT-Spezifikation [SICCT], Abschnitt 4.3.2, und ISO-14443 Teil 4 ([ISO14443-P4]) erfolgen (siehe auch [TIP1-A_2948]).

3.5 Isolation von Verbindungen zum Kartenterminal

TIP1-A_3064 - Kontext der verwalteten Chipkarten
Das eHealth-Kartenterminal MUSS den Kontext der von ihm verwalteten Chipkarten mit Ausnahme des DF.KT-Zugriffs auf eine gSMC-KT lokal zur jeweiligen Verbindung eines Hosts halten.
[<=]

TIP1-A_3065 - Verbindungsabbruch
Das eHealth-Kartenterminal MUSS bei einem Verbindungsabbruch für alle Karten des Terminals, die sich in Verwendung des betroffenen Kontextes befinden, ein Reset der Karten durchführen.
[<=]

3.6 Gleichzeitige Verbindungen zum Kartenterminal

TIP1-A_3066 - Mehrere Verbindungen zu ansteuernden Hosts
Das eHealth-Kartenterminal KANN 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 (siehe [TIP1-A_3067]).

TIP1-A_3068 - Mehrere Verbindungen über SICCT-Port
Das eHealth-Kartenterminal DARF NICHT mehrere Verbindungen über den SICCT-Port unterhalten.
[<=]

TIP1-A_3069 - Verbindungen und eHealth-Kartenterminal
Das eHealth-Kartenterminal MUSS für jede Verbindung, die es unterhält, diese als eigenen Kontext verwalten.
[<=]

TIP1-A_3070 - Ressourcen und unterschiedliche Kontexte
Das eHealth-Kartenterminal MUSS sicherstellen, dass Ressourcen mit Ausnahme des DF.KT im Rahmen des DF.KT-Zugriffs nicht gleichzeitig durch unterschiedliche Kontexte genutzt werden.
[<=]

TIP1-A_3071 - Übergang Nutzungsrecht für Ressourcen
Das eHealth-Kartenterminal MUSS sicherstellen, dass ein Übergang des Nutzungsrechts für Ressourcen zwischen Verbindungs-Kontexten mit Ausnahme des DF.KT im Rahmen des DF.KT-Zugriffs nur in einem sicheren Zustand der jeweiligen Ressourcen (z. B. unmittelbar nach dem Reset einer Chipkarte) gestattet ist.
[<=]

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

TIP1-A_3072 - Verbindung zum Kartenterminal aufgebaut, Ablehnung Konnektorverbindung
Das eHealth-Kartenterminal MUSS bei einer bestehenden Verbindung über eine optionale lokale Schnittstelle jeden Verbindungsversuch eines Konnektors über LAN ablehnen.
[<=]

TIP1-A_3073 - Verbindung zum Kartenterminal aufgebaut, Abbruch Konnektorverbindung
Das eHealth-Kartenterminal MUSS bei einer bestehenden Verbindung über eine optionale lokale Schnittstelle eine eventuell bestehende LAN-Verbindung zu einem Konnektor abbrechen.
[<=]

TIP1-A_3074 - Verbindung zum eHealth-Kartenterminal aufbauen, Zurücksetzten gesteckter Karten
Das eHealth-Kartenterminal MUSS die gesteckten Karten zurücksetzen, wenn eine Verbindung über eine optionale lokale Schnittstelle aufgebaut wird.
[<=]

Dies ist notwendig, um für LAN-Verbindungen zum Konnektor den vertrauenswürdigen Modus zu erhalten, da der lokale Anschluss als unsicher angesehen wird.

3.7 Kartenterminalkommandos

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

TIP1-A_3075 - SICCT-Kommandos über Netzwerk
Das eHealth Kartenterminal MUSS die Kommandos des SICCT-Betriebsmodus der SICCT-Spezifikation [SICCT] verpflichtend für die (Ethernet-) Netzwerk-Schnittstellen des Kartenterminals implementieren.
[<=]

TIP1-A_3077 - Kommandopuffer für APDUs
Das eHealth-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.

3.7.1 Verbindlichkeit des SICCT-Kommandos CONTROL COMMAND

TIP1-A_3251 - „CONTROL COMMAND“-Kommando
Das eHealth-Kartenterminal KANN, abweichend von der SICCT-Spezifikation, das "CONTROL COMMAND"-Kommando nicht implementieren.
[<=]

TIP1-A_3264 - Return Code Control Command
Das eHealth-Kartenterminal MUSS auf das Control Command immer 6200 zurückmelden, falls es gemäß [TIP1-A_3251] nicht umgesetzt wurde.
[<=]

Ein eHealth-Konnektor (oder ein anderes Client-System) darf nicht voraussetzen, dass an ein Terminal übermittelte Kommandos abgebrochen werden können. Da der Erfolg oder Misserfolg eines Abbruchs rein vom Zeitpunkt des Empfangs und der Verarbeitung des Abbruchkommandos abhängig ist, kann auch ein konsistenter Wegfall der Funktionalität akzeptiert werden.

3.7.2 Command EHEALTH TERMINAL AUTHENTICATE

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

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, welches zu dem im Kartenterminal steckenden SM-KT gehört.
3. kann ein Konnektor, der bereits über ein am Kartenterminal eingetragenes Pairing-Geheimnis verfügt, sein Konnektorzertifikat am Kartenterminal bekannt machen und sich dadurch mit dem KT pairen.

3.7.2.1 Funktion

TIP1-A_3078 - Shared Secrets und die öffentlichen Schlüssel
Das eHealth-Kartenterminal MUSS sicherstellen, dass die gespeicherten Shared Secrets und die gespeicherten öffentlichen Schlüssel für Konnektoren eindeutig sind.
[<=]

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 Pairing-Information 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 Pairing-Geheimnisse 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.

Der Ablauf bei der Durchführung der „Kommandosequenz EHEALTH TERMINAL AUTHENTICATE CREATE ‘P2=01’ (SEQ_KT_0001)“ ist im folgenden Aktivitätsdiagramm dargestellt.

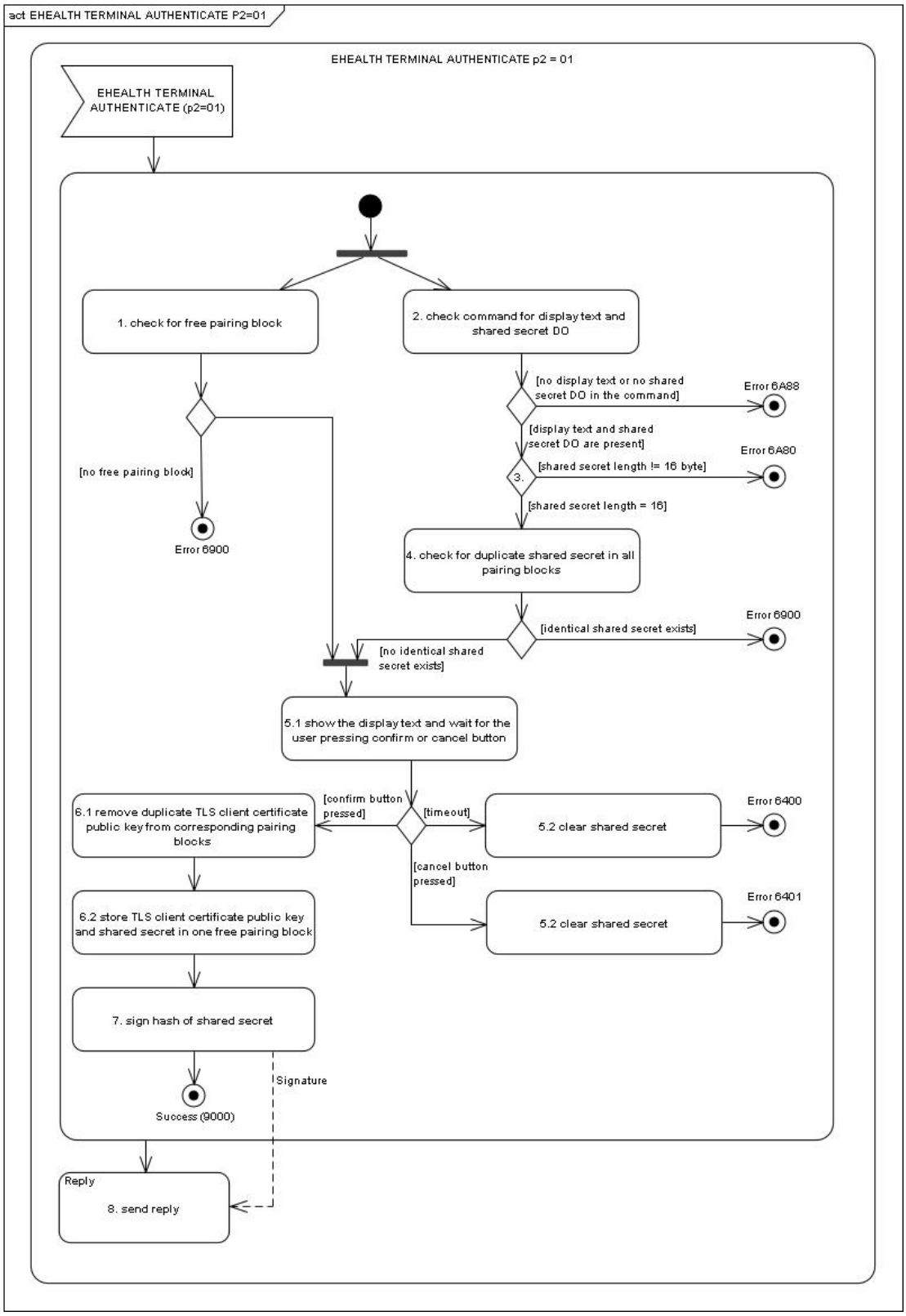


Abbildung 6: Pic_KT_0009 EHEALTH AUTHTENTICATE CREATE

TIP1-A_3125 - Kommando mit P2=’01’ (CREATE)
Das eHealth-Kartenterminal MUSS die Verarbeitung des Kommandos EHEALTH TERMINAL AUTHENTICATE mit P2='01' (CREATE) gemäß Tabelle [gemSpec_KT#SEQ_KT_0001] "Kommandosequenz EHEALTH TERMINAL AUTHENTICATE CREATE P2='01' " implementieren.

[<=]

Tabelle 4: Kommandosequenz EHEALTH TERMINAL AUTHENTICATE CREATE ‘P2=01’ (SEQ_KT_0001)

Schritt Nr.	Beschreibung
1	Das Kartenterminal MUSS prüfen, ob noch ein freier Pairing-Block vorhanden ist. Ist dies nicht der Fall so MUSS das Kartenterminal den Befehl mit einer entsprechenden Fehlermeldung abbrechen (SW1SW2=6900).
2	Das Kartenterminal MUSS prüfen, ob ein Display-Text und ein Shared Secret DO enthalten sind. Fehlt der Display-Text oder das Shared Secret DO, so MUSS das Kommando mit Fehler abbrechen (SW1SW2=6A88).
3	Das Kartenterminal MUSS prüfen, ob der im Shared Secret DO übergebene Byte String genau 16 Byte lang ist. (Shared Secret). Ist dies nicht der Fall, MUSS das Kartenterminal mit Fehler abbrechen (SW1SW2=6A80). Das Shared Secret ist eine vom Konnektor generierte Zufallszahl.
4	Hat es bereits ein identisches Shared Secret gespeichert, MUSS das Kartenterminal mit Fehler abbrechen (SW1SW2=6900).
5	Das Kartenterminal MUSS den Display-Text anzeigen und darauf warten, dass auf dem PIN Pad die Bestätigungs-Taste gedrückt wird. Durch Druck der Abbrechen-Taste MUSS der Befehl abgebrochen werden. Wird nicht binnen einer herstellerspezifischen Zeitspanne die NICHT größer als 10 Minuten sein DARF, die Bestätigungs-Taste gedrückt, MUSS der Befehl abgebrochen werden. Bei Abbruch MUSS das Kartenterminal das Shared Secret wieder aus seinem Speicher löschen und eine Fehlermeldung zurückschicken. Bei Abbruch durch Tastendruck MUSS mit Fehlercode SW1SW2=6401 geantwortet werden. Bei Abbruch durch Timeout MUSS mit Fehlercode SW1SW2=6400 geantwortet werden.
6	Hat das Kartenterminal den öffentlichen Schlüssel des beim Verbindungsaufbau präsentierten Konnektorzertifikats bereits gespeichert, MUSS es diesen aus dem korrespondierenden Pairing-Block löschen. Der Pairing-Block MUSS jedenfalls erhalten bleiben, selbst wenn keine öffentlichen Schlüssel in ihm gespeichert sind. Das Kartenterminal MUSS den im Shared Secret DO übergebenen Byte-String zusammen mit dem während des TLS-Aufbaus erhaltenen öffentlichen Schlüssel des Konnektorzertifikats in einem unbenutzten Pairing-Block abspeichern.
7	Für das erhaltene Shared Secret wird mittels des SM-KT unter Verwendung des Zertifikats für die SMKT-Identität eine Signatur erstellt. Hierfür MUSS das Kartenterminal den SHA-256-Hash-Wert des Shared Secrets generieren. Dieser Hash-Wert MUSS durch das SM-KT mit dem in [gemSpec_Krypt#GS-A_5207] festgelegten Verfahren signiert werden. Dieses Verfahren steht auf dem SM-KT zur Verfügung.
8	Die in Schritt 7 berechnete Signatur MUSS in der Response-APDU zurückgeschickt werden.

Der Ablauf bei der Durchführung der EHEALTH TERMINAL AUTHENTICATE VALIDATE Kommandosequenz SEQ_KT_0002 ist im folgenden Aktivitätsdiagramm zusammenfassend dargestellt.

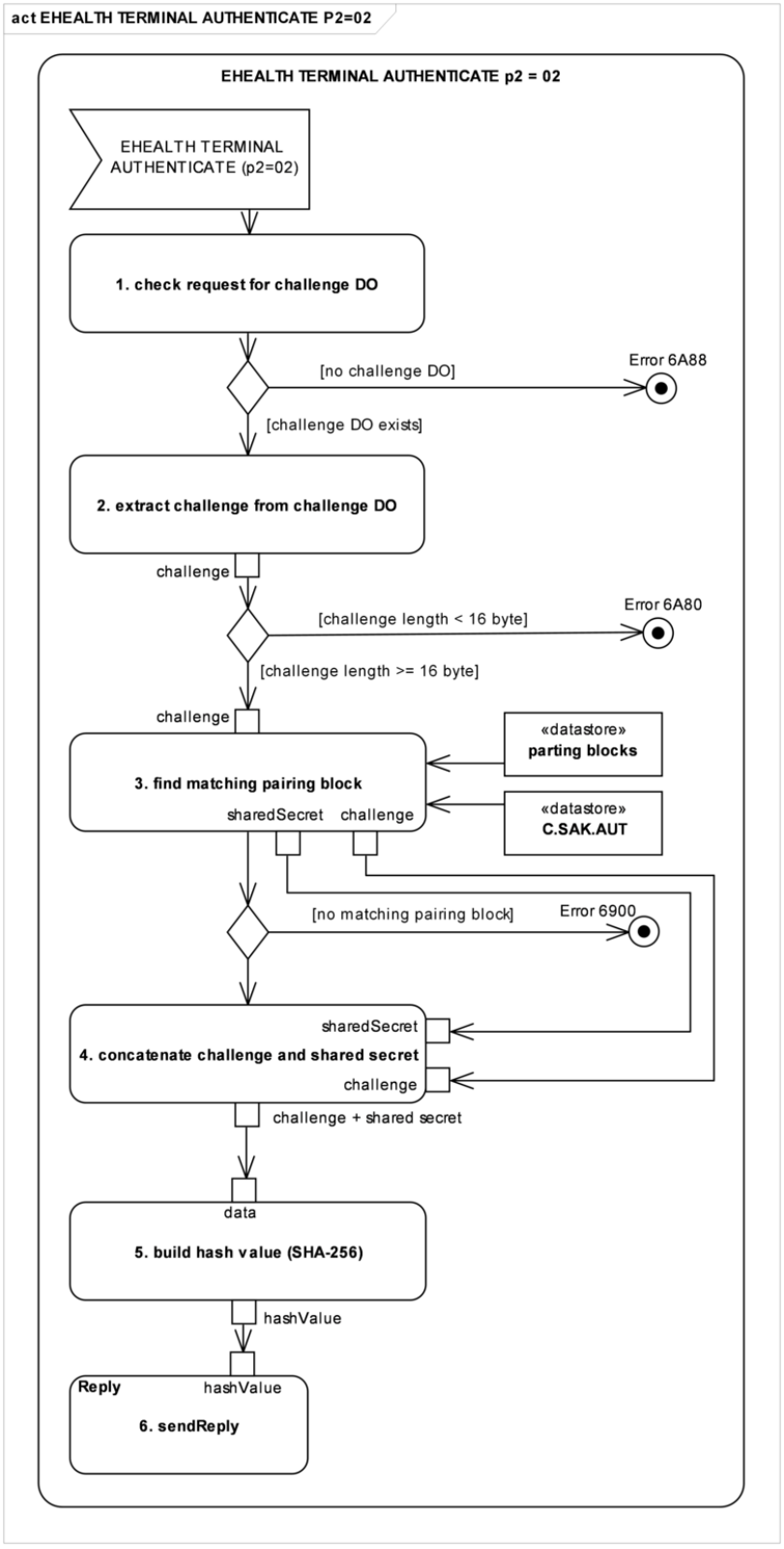


Abbildung 7: Pic_KT_0010 EHEALTH AUTHTENTICATE VALIDATE

TIP1-A_3126 - Kommando mit P2=’02’ (VALIDATE)
Das eHealth-Kartenterminal MUSS die Verarbeitung des Kommandos EHEALTH TERMINAL AUTHENTICATE mit P2='02' (VALIDATE) gemäß Tabelle [gemSpec_KT#SEQ_KT_0002] "Kommandosequenz EHEALTH TERMINAL AUTHENTICATE VALIDATE P2='02'" implementieren.

[<=]

Tabelle 5: Kommandosequenz EHEALTH TERMINAL AUTHENTICATE VALIDATE ‘P2=02’ (SEQ_KT_0002)

Schritt Nr.	Beschreibung
1	Das Kartenterminal MUSS prüfen, ob ein Shared Secret Challenge DO enthalten ist. Fehlt das Shared Secret Challenge DO, so MUSS das Kartenterminal das Kommando mit Fehler abbrechen (SW1SW2=6A88).
2	Das Kartenterminal MUSS prüfen, ob der im Shared Secret Challenge DO übergebene Byte-String mindestens 16 Byte lang ist. Ist dies nicht der Fall MUSS das Kartenterminal das Kommando mit Fehler abbrechen (SW1SW2=6A80).
3	Das Kartenterminal MUSS anhand des öffentlichen Schlüssels des Konnektorzertifikats den Pairing-Block, der das korrespondierende Shared Secret enthält, suchen. Hierfür ist ein byteweiser Vergleich der Schlüssel ausreichend. Hat das Kartenterminal den öffentlichen Schlüssel noch nicht gespeichert, MUSS es mit einer Fehlermeldung abbrechen (SW1SW2=6900).
4	Hat das Kartenterminal in Schritt 3 ein korrespondierendes Shared Secret gefunden, MUSS es an die Shared Secret Challenge das korrespondierende Shared Secret anhängen.
5	Von diesem in Schritt 4 generierten Array MUSS der SHA-256-Hash-Wert berechnet werden.
6	Der berechnete Hash-Wert MUSS in der Response-APDU an den Konnektor zurückgeschickt werden.
7	Falls eine Display Message angegeben wurde, MUSS diese ignoriert werden.

Falls das Kommando mit P2=’03’ oder P2=’04’ (ADD) ausgeführt wird so läuft die Verarbeitung des Kommandos im Kartenterminal in 2 Phasen ab (siehe Kapitel 2.5.2.4). In der ersten Phase fordert der Konnektor vom Kartenterminal eine Challenge ab, um in der zweiten Phase die Kenntnis des Shared Secrets nachweisen zu können.

Der Ablauf bei der Durchführung der EHEALTH TERMINAL AUTHENTICATE ADD Phase 1 Kommandosequenz aus Tabelle 6 „SEQ_KT_0003“ ist im folgenden Aktivitätsdiagramm zusammenfassend dargestellt.

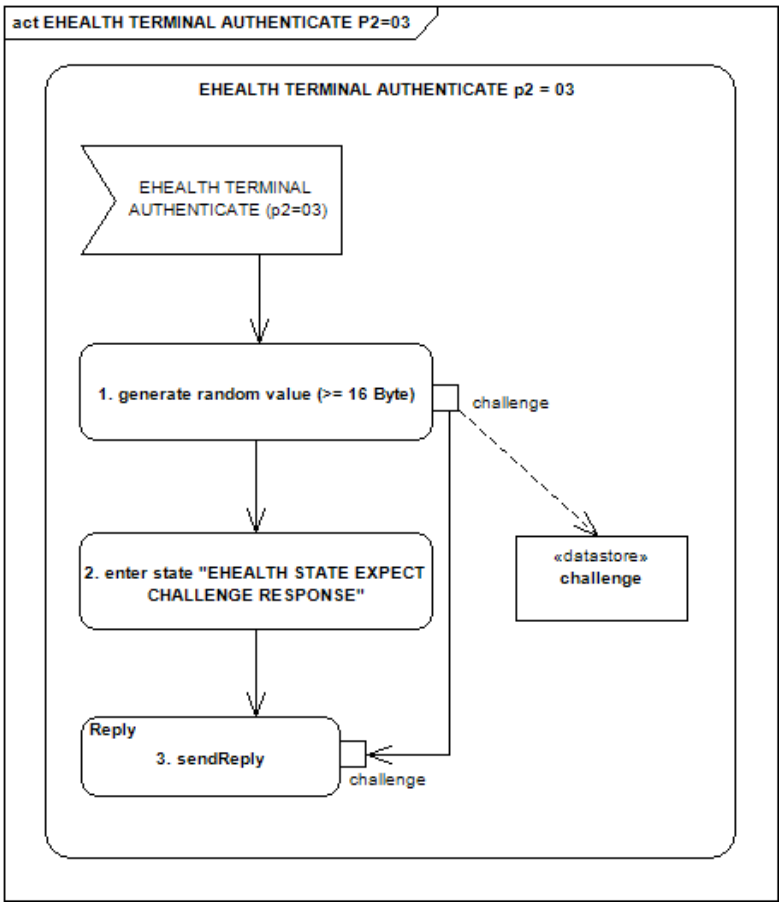


Abbildung 8: Pic_KT_0011 EHEALTH AUTHENTICATE - ADD Phase 1

TIP1-A_3127 - P2=’03’ (ADD Phase 1)
Das eHealth-Kartenterminal MUSS die Verarbeitung des Kommandos EHEALTH TERMINAL AUTHENTICATE mit P2='03' (ADD Phase 1) gemäß Tabelle [gemSpec_KT#SEQ_KT_0003] "Kommandosequenz EHEALTH TERMINAL AUTHENTICATE ADD Phase 1 P2='03'" implementieren.

[<=]

Tabelle 5: Kommandosequenz EHEALTH TERMINAL AUTHENTICATE ADD Phase 1 ‘P2=03’ (SEQ_KT_0003)

Schritt Nr.	Beschreibung
1	Das Kartenterminal MUSS mittels des Zufallszahlengenerators des SM-KT eine Zufallszahl erzeugen, deren Länge dem Wert des Parameters Le aus dem empfangenen Kommando EHEALTH TERMINAL AUTHENTICATE entspricht. Die Zufallszahl MUSS mindestens 16 Byte lang sein.
2	Das Kartenterminal MUSS in den Zustand „EHEALTH STATE EXPECT CHALLENGE RESPONSE“ übergehen und die Zufallszahl auslesegeschützt abspeichern.
3	Das Kartenterminal MUSS die in Schritt 1 generierte Zufallszahl in der Response-APDU an den Konnektor zurücksenden.

Der Ablauf bei der Durchführung der EHEALTH TERMINAL AUTHENTICATE ADD Phase 2 Kommandosequenz SEQ_KT_0004 ist im folgenden Aktivitätsdiagramm zusammenfassend dargestellt.

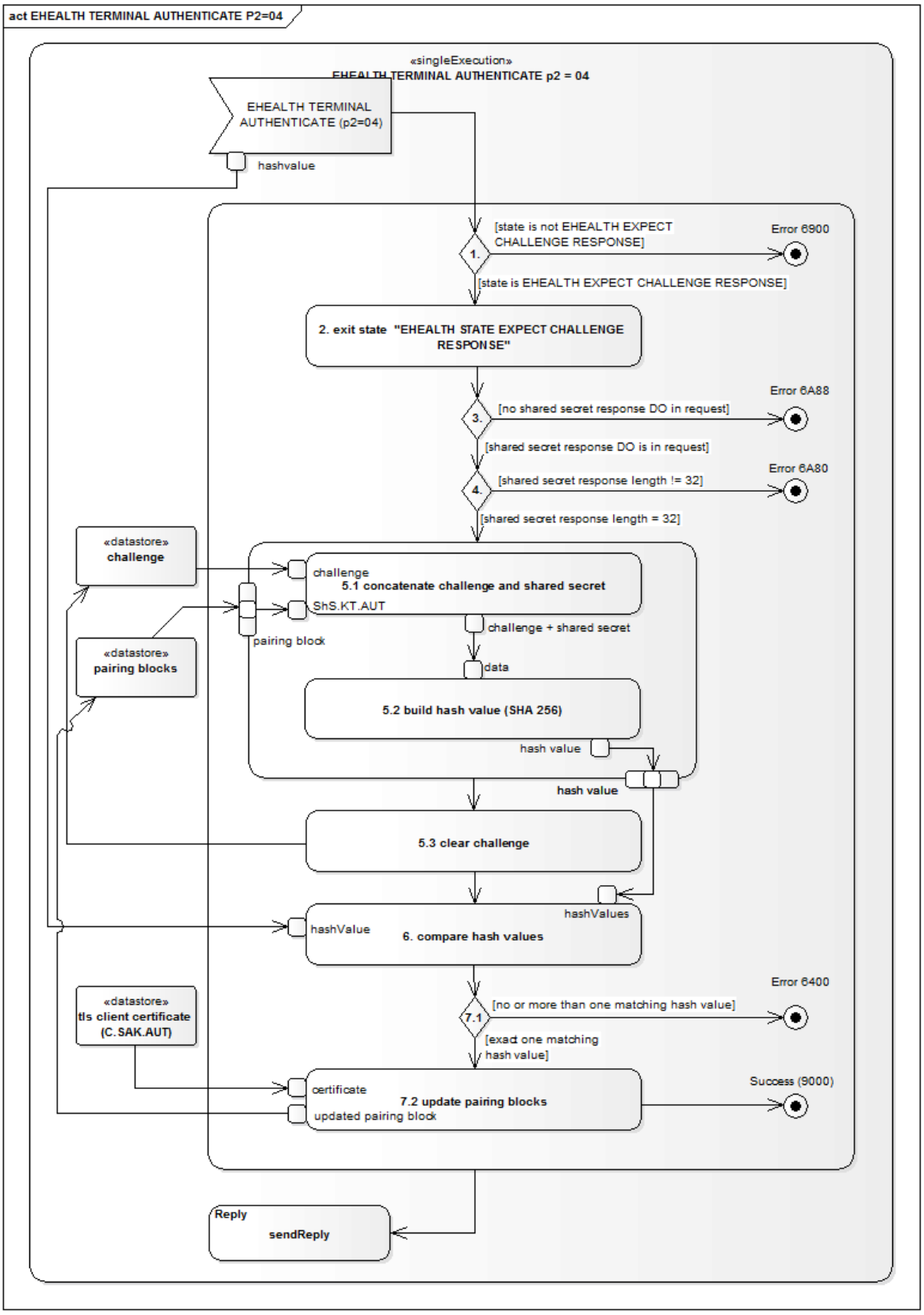


Abbildung 9: Pic_KT_0012 EHEALTH AUTHENTICATE - ADD Phase 2

TIP1-A_3128 - P2=’04’ (ADD Phase 2)
Das eHealth-Kartenterminal MUSS die Verarbeitung des Kommandos EHEALTH TERMINAL AUTHENTICATE mit P2='04' (ADD Phase 2) gemäß Tabelle [gemSpec_KT#SEQ_KT_0004] "Kommandosequenz EHEALTH TERMINAL AUTHENTICATE ADD Phase 2 P2='04'" implementieren.

[<=]

Tabelle 6: Kommandosequenz EHEALTH TERMINAL AUTHENTICATE ADD Phase 2 ‘P2=04’ (SEQ_KT_0004)

Schritt Nr.	Beschreibung
1	Das Kartenterminal MUSS prüfen, ob es sich im Zustand „EHEALTH STATE EXPECT CHALLENGE RESPONSE“ befindet. Ist dies nicht der Fall, MUSS das Kartenterminal das Kommando mit einem Fehler abbrechen (SW1SW2=6900).
2	Das Kartenterminal MUSS den Zustand „EHEALTH STATE EXPECT CHALLENGE RESPONSE“ verlassen.
3	Das Kartenterminal MUSS prüfen, ob ein Shared Secret Response DO enthalten ist. Fehlt das Shared Secret Response DO, so MUSS das Kartenterminal das Kommando mit Fehler abbrechen (SW1SW2=6A88).
4	Das Kartenterminal MUSS prüfen, ob der im Shared Secret Response DO übergebene Byte-String genau 32 Byte lang ist. Ist dies nicht der Fall, MUSS das Kartenterminal das Kommando mit Fehler abbrechen (SW1SW2=6A80)
5	Für jeden genutzten Pairing-Block MUSS das Kartenterminal aus der in Phase 1 generierten Zufallszahl und dem Shared Secret des jeweiligen Pairing-Blocks die SHA-256 Hash-Werte (vgl. Ablauf bei P2=’02’) berechnen und anschließend die generierte Zufallszahl löschen.
6	Das Kartenterminal MUSS alle generierten Hash-Werte mit der im Shared Secret Response DO enthaltenen Antwort des Konnektors vergleichen.
7	Stimmt genau einer der Hash-Werte überein, MUSS das Kartenterminal den Pairing-Block, der das erfolgreich geprüfte Shared Secret enthält, selektieren und dort den öffentlichen Schlüssel des beim TLS-Verbindungsaufbaus erhaltenen Konnektorzertifikats eintragen. Sonst MUSS das Kartenterminal das Kommando mit Fehler abbrechen (SW1SW2=6400). Ist der neue öffentliche Schlüssel bereits in einem anderen Pairing-Block als dem selektierten enthalten, MUSS das Kartenterminal diesen, vor dem Eintragen des neuen Schlüssels aus dem entsprechenden Pairing-Block löschen. Die Regeln für das Eintragen des neuen öffentlichen Schlüssels sind dabei wie folgt: • Ist der neue öffentliche Schlüssel bereits im selektierten Pairing-Block enthalten, DARF das Kartenterminal den Schlüssel NICHT eintragen und mit einem Command Successful (SW1SW2=9000) antworten. • Ist der neue öffentliche Schlüssel noch nicht im selektierten Pairing-Block enthalten und ist noch mindestens ein Speicherslot für öffentliche Schlüssel im Pairing-Block frei, MUSS der neue öffentliche Schlüssel hinzugefügt werden und das Kartenterminal mit einem Command Successful (SW1SW2=9000) antworten.

	• Ist der neue öffentliche Schlüssel noch nicht im selektierten Pairing-Block enthalten und ist kein Speicherslot für öffentliche Schlüssel im Pairing-Block mehr frei, MUSS der älteste öffentliche Schlüssel, jener dessen Pairing-Vorgang am längsten zurück liegt, mit dem neuen öffentlichen Schlüssel überschrieben werden und das Kartenterminal mit einem Command Successful (SW1SW2=9000) antworten.

3.7.2.2 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 und ist in Abbildung „Pic_KT_0013 Zustandsdiagramm EHEALTH EXPECT CHALLENGE RESPONSE“ dargestellt.

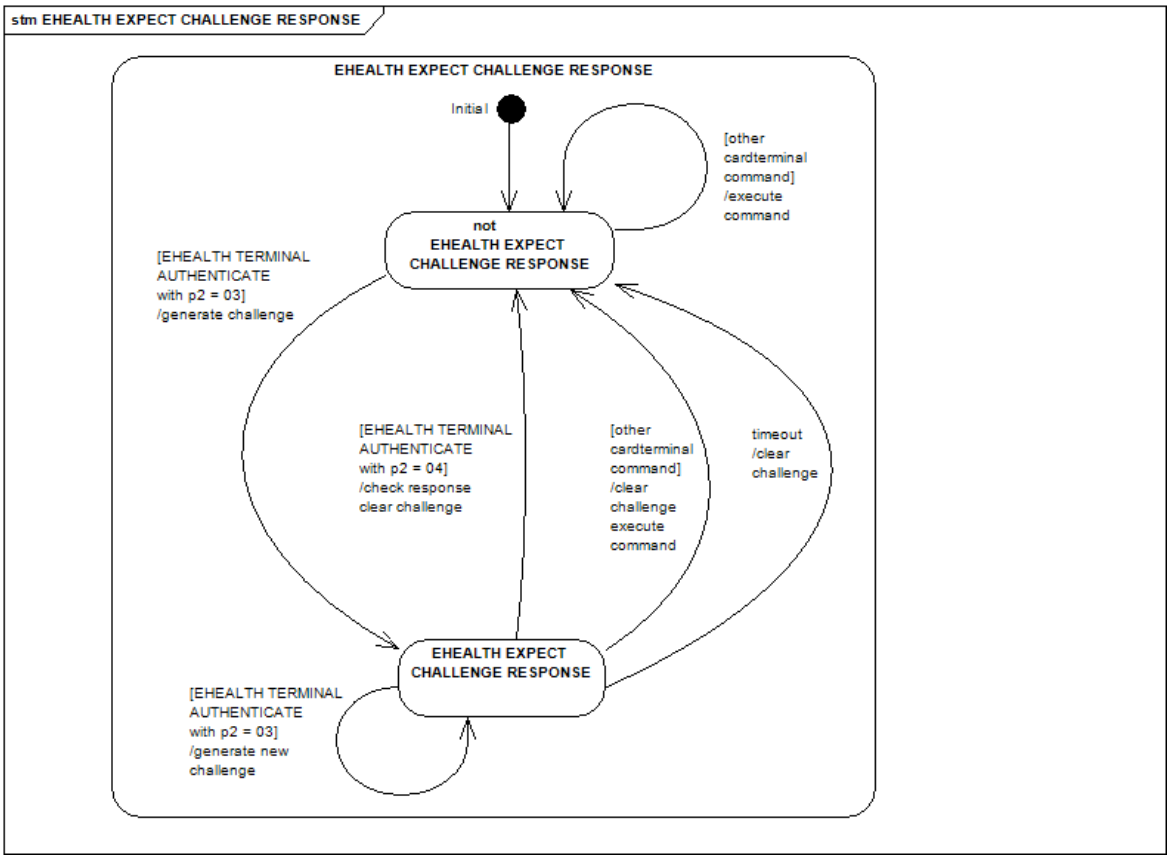


Abbildung 10: Pic_KT_0013 Zustandsdiagramm EHEALTH EXPECT CHALLENGE RESPONSE

TIP1-A_3113 - Zustand EHEALTH EXPECT CHALLENGE RESPONSE, Abbruch durch anderes Kommando

Das eHealth-Kartenterminal MUSS den Zustand EHEALTH EXPECT CHALLENGE RESPONSE 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.
[<=]

TIP1-A_3114 - Zustand EHEALTH EXPECT CHALLENGE RESPONSE, Einnehmen des Zustands
Das eHealth-Kartenterminal MUSS sicherstellen, dass es den Zustand EHEALTH EXPECT CHALLENGE RESPONSE nur durch den Befehl EHEALTH TERMINAL AUTHENTICATE mit (P2='03') einnehmen kann.
[<=]

TIP1-A_3115 - Zustand EHEALTH EXPECT CHALLENGE RESPONSE, Timeout
Das eHealth-Kartenterminal MUSS den Zustand EHEALTH EXPECT CHALLENGE RESPONSE nach maximal 30 Sek. verlieren und dabei auch die generierte Challenge löschen.
[<=]

3.7.2.3 Anwendungsbedingungen

TIP1-A_3116 - SICCT-Modus und EHEALTH EXPECT CHALLENGE RESPONSE
Das eHealth-Kartenterminal MUSS sich im SICCT-Betriebsmodus gemäß [SICCT#5.5.7] befinden, um das Kommando EHEALTH TERMINAL AUTHENTICATE auszuführen.
[<=]

TIP1-A_3177 - Ausführung des Kommandos EHEALTH TERMINAL AUTHENTICATE
Das eHealth-Kartenterminal MUSS die Ausführung des Kommandos EHEALTH TERMINAL AUTHENTICATE sowohl in einer CT ADMIN Session als auch in einer CT CONTROL Session ermöglichen.
[<=]

3.7.2.4 Command Structure

TIP1-A_3119 - Kommandostruktur des EHEALTH TERMINAL AUTHENTICATE Kommandos
Das eHealth-Kartenterminal MUSS die Kommandostruktur des EHEALTH TERMINAL AUTHENTICATE-Kommandos wie in Tabelle [gemSpec_KT#CMD_KT_0001] „Command Definition EHEALTH TERMINAL AUTHENTICATE" beschrieben implementieren.

[<=]

Tabelle 7: Command Definition EHEALTH TERMINAL AUTHENTICATE (CMD_KT_0001)

EHEALTH Kommando	Codierung 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	Referenced Coding	
		’FF’	Escape : Signal Referenced Coding of P1 Functional Unit referenced by Functional Unit Index Data Object (FUI DO) contained within Command Data Field.
	bit8 .. bit1	Direct Coding (mandatory)	
		’00’	Address Cardterminal
P2	Command Qualifier		
	bit8..bit1	’01’	create pairing block for new Shared Secret and Konnektor
		’02’	authenticate with Shared Secret
		‘03’	generate Challenge
		’04’	add Konnektor to known pairing block
		other values RFU	
Lc	Length of Command Data Nc		
	Direct coding (mandatory)		
	P2=01	Lc short; ’12’<=Lc<=’FF’	
	P2=02	Lc short; ’12’<=Lc<=’81’	
	P2=03	absent	
	P2=04	Lc short Lc=’22’	
	Referenced Coding		
	P2=01	Lc short; ’16’<=Lc<=’FF’	
	P2=02	Lc short; ’16’<= Lc<= ’85’	
	P2=03	Lc short; Lc=’04’	
	P2=04	Lc short; Lc=’26’	
Data	Command Data		
	In case of Direct Coding of ’P1’ (mandatory)		
	In Case of P2=01		

	Shared Secret DO	Byte sequence: Shared secret generated by Konnektor during pairing	see Chapter 3.7.2.7
	APPLICATION LABEL DO	Text / display Message	see SICCT 5.5.10.19
	SICCT Message To Be displayed DO	Constructed TLV-DO containing 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 3.7.2.8
	In Case of P2=03: absent		
	In Case of P2=04		
	Shared Secret Response DO	SHA-256 Hashvalue	see Chapter 3.7.2.9
	In case of Referenced Coding of 'P1'		
	FUI DO	'84020000'	Functional Unit Index Data Object
	In Case of P2=01		
	Shared Secret DO	Byte sequence: Shared secret generated by Konnektor during pairing	see Chapter 3.7.2.7
	APPLICATION LABEL DO	Text / display Message	see SICCT 5.5.10.19
	SICCT Message To Be displayed DO	Constructed TLV-DO containing 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 3.7.2.8
	In Case of P2=03: absent		
	In Case of P2=04		
	Shared Secret Response DO	SHA-256 Hashvalue	see Chapter 3.7.2.9
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		

3.7.2.5 Response Structure

TIP1-A_3120 - Antwortstruktur des EHEALTH TERMINAL AUTHENTICATE Kommandos

Das eHealth-Kartenterminal MUSS die Antwortstruktur des EHEALTH TERMINAL AUTHENTICATE Kommandos wie in Tabelle [gemSpec_KT#CMD_KT_0002] „EHEALTH AUTHENTICATE Response Structure Definition" implementieren.

[<=]

Tabelle 8: EHEALTH AUTHENTICATE Response Structure Definition (CMD_KT_0002)

EHEALTH TERMINAL AUTHENTICATE	Codierung 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		
	Requested data	in case of success and P2=03: Challenge		
	Empty	in case of success and P2=04 or in case of error		

3.7.2.6 Status-Codes SW1-SW2

TIP1-A_3121 - Allgemeine Status Codes gemäß SICCT-Spezifikation

Das eHealth-Kartenterminal MUSS zusätzlich zu den allgemeinen Status Codes gemäß SICCT-Spezifikation die kommandospezifischen Status Codes gemäß [gemSpec_KT#CMD_KT_0003] „EHEALTH AUTHENTICATE Status Code Definition" implementieren.

[<=]

Tabelle 9: EHEALTH AUTHENTICATE Status Code Definition (CMD_KT_0003)

SW1SW2	P2	Specification	Meaning
6400	‘01’ CREATE	Execution Error	Nor or incomplete input in time
	‘04’ ADD	Execution Error	Hash value not found
6401	‘01’ CREATE	Execution Error	Process aborted by pressing of CANCEL key

6900	‘01’ CREATE	Command not allowed	No unused pairing block available or shared secret already stored
	‘02’ VALIDATE	Command not allowed	Presented Public Key unknown
	‘04’ ADD	Command not allowed	CT is not in the state “EHEALTH EXPECT CHALLENGE RESPONSE”
6901	‘01’ CREATE	Command not allowed	No matching TSP certificate
	‘02’ VALIDATE	Command not allowed	No matching TSP certificate
	‘04’ ADD	Command not allowed	No matching TSP certificate
6A80	‘01’ CREATE	Incorrect Parameters	Length of SS DO is not 16 bytes or no display message given.
	‘02’ VALIDATE	Incorrect Parameters	Length of SSC DO is smaller than 16 bytes
	’04’ ADD	Incorrect Parameters	Length of SSR DO is unequal 32 bytes

3.7.2.7 Shared Secret Data Object

Das Shared Secret Data Object enthält das vom Konnektor während des Pairing-Vorgangs generierte Shared Secret.

TIP1-A_3122 - “Shared Secret Data Object Definition”
Das eHealth-Kartenterminal MUSS das Shared Secret Data Object gemäß [gemSpec_KT#DO_KT_0003] "Shared Secret Data Object Definition" implementieren.

[<=]

Tabelle 10: Shared Secret Data Object Definition (DO_KT_0003)

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

3.7.2.8 Shared Secret Challenge Data Object

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

TIP1-A_3123 - "Shared Secret Data Object Challenge Definition"
Das eHealth-Kartenterminal MUSS das Shared Secret Data Challenge Object gemäß [gemSpec_KT#DO_KT_0004] "Shared Secret Data Object Challenge Definition" implementieren.

[<=]

Tabelle 11: Shared Secret Challenge Data Object Definition (DO_KT_0004)

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		

3.7.2.9 Shared Secret Response Data Object

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

TIP1-A_3124 - "Shared Secret Data Object Response Definition"
Das eHealth-Kartenterminal MUSS das Shared Secret Data Response Object gemäß [gemSpec_KT#DO_KT_0005] "Shared Secret Data Object Response Definition" implementieren.

[<=]

Tabelle 12: Shared Secret Response Data Object Definition (DO_KT_0005)

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	
	'20'	one byte coding LEN=32
	all other values	reject with error
VALUE	Shared Secret Response	
	SHA-256 Hashvalue	

3.7.3 Ergänzung der Commands SICCT OUTPUT und SICCT INPUT

TIP1-A_3079 - SICCT OUTPUT und SICCT INPUT Displaynachricht
Das eHealth-Kartenterminal MUSS die mittels SICCT OUTPUT und SICCT INPUT übergebene Displaynachricht gemäß [SICCT] zur Anzeige bringen können.
[<=]

TIP1-A_3080 - SICCT OUTPUT und SICCT INPUT mindestens 48 Zeichen
Das eHealth-Kartenterminal MUSS bei der Anzeige von Displaynachrichten, die mittels SICCT OUTPUT und SICCT INPUT übergeben werden, mindestens die Länge von 48 Zeichen einer Displaynachricht unterstützen.
[<=]

3.7.4 Ergänzung der Commands SICCT REQUEST ICC und SICCT EJECT ICC

TIP1-A_3081 - SICCT REQUEST ICC und SICCT EJECT ICC Displaynachricht
Das eHealth-Kartenterminal MUSS die mittels SICCT REQUEST ICC und SICCT EJECT ICC übergebene Displaynachricht gemäß [SICCT] zur Anzeige bringen können.
[<=]

TIP1-A_3082 - SICCT REQUEST ICC und SICCT EJECT ICC mindestens 48 Zeichen
Das eHealth-Kartenterminal MUSS bei der Anzeige von Displaynachrichten, die mittels SICCT REQUEST ICC und SICCT EJECT ICC übergeben werden, mindestens die Länge von 48 Zeichen einer Displaynachricht unterstützen.
[<=]

3.7.5 Ergänzung des Command SICCT PERFORM VERIFICATION

TIP1-A_3083 - SICCT PERFORM VERIFICATION: Parameter Displaynachricht und PIN-Prompt
Das eHealth-Kartenterminal MUSS die mittels SICCT PERFORM VERIFICATION übergebenen Parameter Displaynachricht und PIN-Prompt gemäß [SICCT#5.6.1] zur Anzeige bringen können.
[<=]

TIP1-A_3084 - Displaynachrichten mittels SICCT PERFORM VERIFICATION
Das eHealth-Kartenterminal MUSS bei der Anzeige von Displaynachrichten, die mittels SICCT PERFORM VERIFICATION übergeben werden, mindestens die Länge von 48 Zeichen einer Displaynachricht unterstützen.
[<=]

TIP1-A_3085 - Anzeige von PIN-Prompts mittels SICCT PERFORM VERIFICATION

Das eHealth-Kartenterminal MUSS bei der Anzeige von PIN-Prompts, die mittels SICCT PERFORM VERIFICATION übergeben werden, mindestens die Länge von 10 Zeichen eines PIN-Prompts unterstützen.
[<=]

TIP1-A_3086 - SICCT PERFORM VERIFICATION Kommando, Eingabe des 1. Zeichens
Das eHealth-Kartenterminal MUSS bei dem Kommando SICCT PERFORM VERIFICATION, abweichend von der SICCT-Spezifikation, als Standard 30 Sekunden auf die Eingabe des ersten Zeichens oder Betätigung der Abbruchtaste warten.
[<=]

TIP1-A_3087 - SICCT PERFORM VERIFICATION Kommando, Eingabe der weiteren Zeichen
Das eHealth-Kartenterminal MUSS bei dem Kommando SICCT PERFORM VERIFICATION, abweichend von der SICCT-Spezifikation, als Standard 30 Sekunden auf die Eingabe des jeweils nächsten Zeichens oder der Betätigung der Abbruch- bzw. Bestätigungstaste warten.
[<=]

3.7.6 Ergänzung des Command SICCT MODIFY VERIFICATION DATA

TIP1-A_6483 - SICCT MODIFY VERIFICATION DATA Displaynachricht und PIN-Prompt
Das eHealth-Kartenterminal SOLL die mittels SICCT MODIFY VERIFICATION DATA übergebenen Parameter Displaynachricht und PIN-Prompt gemäß [SICCT#5.6.1] zur Anzeige bringen können und dabei die Mindestlängen der Displaynachricht und des PIN-Prompts analog zu [TIP1-A_3084] und [TIP1-A_3085] unterstützen.
[<=]

Nur bei eHealth-Kartenterminals, die auf bereits zugelassenen eHealth-BCS-Geräten basieren und bei denen die Umstellung vom eHealth-BCS-Spezifikationsstand auf den eHealth-Spezifikationsstand per Firmware Upgrade (Firmware Update) erfolgt, kann eine Nichterfüllung der Anforderung [TIP1-A_6483] akzeptiert werden.

TIP1-A_3088 - SICCT MODIFY VERIFICATION DATA Kommando, Eingabe des 1. Zeichens
Das eHealth-Kartenterminal MUSS bei dem Kommando SICCT MODIFY VERIFICATION, abweichend von der SICCT-Spezifikation, als Standard 30 Sekunden auf die Eingabe des ersten Zeichens oder Betätigung der Abbruchtaste warten.
[<=]

TIP1-A_3089 - SICCT MODIFY VERIFICATION DATA Kommando, Eingabe der weiteren Zeichen
Das eHealth-Kartenterminal MUSS bei dem Kommando SICCT MODIFY VERIFICATION, abweichend von der SICCT-Spezifikation, als Standard 30 Sekunden auf die Eingabe des jeweils nächsten Zeichens oder der Betätigung der Abbruch- bzw. Bestätigungstaste warten.
[<=]

3.7.7 Änderungen des Card Terminal Manufacturer Data Objects

TIP1-A_3948 - CTM Festlegung für eHealth
Abweichend zu Kapitel 5.5.10.6 der SICCT-Spezifikation MUSS das eHealth-Kartenterminal im Card Terminal Manufacturer Data Object (CTM DO) im Feld „CTM“ (Cardterminal Manufacturer) das von der gematik vergebene Herstellerkürzel zurückgeben.
[<=]

TIP1-A_3131 - Ergänzung der SICCT-Spezifikation
Das eHealth-Kartenterminal MUSS, ergänzend zu Kapitel 5.5.10.6 der SICCT-Spezifikation, das CardTerminal Manufacturer Data Object CTM DO so implementieren, dass es verpflichtend über das Discretionary Data Data Object (DD DO) verfügt.
[<=]

TIP1-A_3118 - Discretionary Data Data Object
Das eHealth-Kartenterminal MUSS das Discretionary Data Data Object wie in [gemSpec_KT#DO_KT_0001] „Discretionary Data Data Object Definition" und [gemSpec_KT#DO_KT_0002] „Discretionary Data Data Object Type Definition" implementieren.

[<=]

Tabelle 13: Discretionary Data Data Object Definition (DO_KT_0001)

Discretionary Data Data Object (DD DO)				
TAG	‘D7’	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 = 23 (‘17’)		
LEN	LEN coding see SICCT 5.5.10.3			
	51 <=LEN<=110			
VALUE	DO name		length	Description
	VER	man	9	EHEALTH-Interface version reflecting the conformance to specific versions of applicable gematik interface specifications.
	PT	man	2	Producttype
	PTV	man	9	Producttype Version
	MODN	man	8	Model Name of Cardterminal
	FWV	man	9	Firmware Version
	HWV	man	9	Hardware Version
	FWG	man	5	Version of Firmware

				Group
	VEN	opt	0..59	Vendor specific information

Tabelle 14: Discretionary Data Data Object Type Definition (DO_KT_0002)

Data	Len		Description
VER	9	man	9 Byte ASCII String of form [XXX][YYY][ZZZ] The values are defined as follows (see also [gemSpec_OM#2.1.2]) XXX Major Version number left-padded with space ‘20’ YYY Minor version number left-padded with space ‘20’ ZZZ Revision number left-padded with space ‘20’ The interface version is issued by the gematik Example: The interface version 2.61.242 (2 Major, 61 Minor, 242 Revision) yields the ASCII encoded string: ‘202032203631323432’
PT	2	man	Producttype ‘KT’ 2 Byte ASCII String with the following content: The name of the producttyp (KT) yields the ASCII encoded string: ‘4B54’
PTV	9	man	Producttype Version 9 Byte ASCII String of form [XXX][YYY][ZZZ] XXX Major Version number left-padded with space ‘20’ YYY Minor version number left-padded with space ‘20’ ZZZ Revision number left-padded with space ‘20’ Example: The firmware version 2.61.242 (2 Major, 61 Minor, 242 Revision) yields the ASCII encoded string: ‘202032203631323432’
MODN	8	man	8 Byte ASCII String- left-padded with Space (‘20’) Named as ”Produktkürzel” in [gemSpec_OM] Vendor specific
FWV	9	man	Firmware Version 9 Byte ASCII String of form [XXX][YYY][ZZZ] XXX Major Version number left-padded with space ‘20’ YYY Minor version number left-padded with space ‘20’ ZZZ Revision number left-padded with space ‘20’ Example: The firmware version 2.61.242 (2 Major, 61 Minor, 242 Revision) yields the ASCII encoded string: ‘202032203631323432’
HWV	9	man	Hardware Version 9 Byte ASCII String of form [XXX][YYY][ZZZ] XXX Major Version number left-padded with space ‘20’ YYY Minor version number left-padded with space ‘20’ ZZZ Revision number left-padded with space ‘20’ Example: The hardware version 2.61.242 (2 Major, 61 Minor, 242 Revision)

			yields the ASCII encoded string: ‘202032203631323432’
FWG	5	man	Firmware Group Version 5 Byte ASCII String Format defined in [gemSpec_KSR]
VEN	0..59	opt.	Optional, vendor specific coded string.

Die für eine konkrete EHEALTH-Schnittstellenversion des Kartenterminals gültige Versionsnummer (VER) ist dem Produkttypsteckbrief zu entnehmen (siehe auch Kapitel 2.3.12.2). Die Versionsnummern werden nach den in [gemSpec_OM#2.2] spezifizierten Vorgaben vergeben.

3.7.8 Ergänzung zu Service Discovery/Announcement

TIP1-A_3151 - UNICast basierte Dienstanfragepakete
Das eHealth-Kartenterminal MUSS zusätzlich zu den in [SICCT#6.1.3.1] definierten Verfahren auch UNICast-basierte Dienstanfragepakete empfangen und verarbeiten können und diese mit einem Dienstbeschreibungspaket beantworten.
[<=]

TIP1-A_3265 - Ergänzung Sicherheitsprotokolle
Das eHealth-Kartenterminal MUSS ergänzend zur [SICCT] die Werte gemäß [gemSpec_KT#DO_KT_0006] für das Datenfeld "Sicherheitsprotokoll" im Dienstbeschreibungspaket implementieren.
[<=]

Tabelle 15: Sicherheitsprotokolle (DO_KT_0006)

Protokoll	Tag (hex.)	Datenlänge (Bytes)	Daten	Wert (hex.)	Beschreibung
TLS	’8A’	1	Unterstützte Protokollversion (1 Byte)	’10’	TLS 1.0 [RFC2246]
				’11’	TLS 1.0 [RFC2246] + AES TLS Erweiterungen [RFC5248]
				’20’	TLS 1.1 [RFC4346]
				’30’	TLS 1.2 [RFC5246]

3.7.9 Ergänzung des Command SICCT INIT CT SESSION

TIP1-A_3184 - KT-Unterstützung des anonymen Zugriffs für Rolle CT CONTROL
Das eHealth-Kartenterminal MUSS ergänzend zur Spezifikation des Kommandos „SICCT INIT CT SESSION" der SICCT-Spezifikation den anonymen Zugriff für die Rolle CT CONTROL unterstützen.
[<=]

TIP1-A_3191 - Definition anonyme Session
Das eHealth-Kartenterminal MUSS den anonymen Zugriff gemäß [TIP1-A_3184] mit leeren Datenobjekten (Tag '13') mit der Länge Null für Benutzernamen und Passwort implementieren.
[<=]

3.7.10 Verbindlichkeit des SICCT-Kommandos SICCT SELECT CT MODE

TIP1-A_3012 - Streichung "SICCT SELECT CT MODE"
Das eHealth-Kartenterminal DARF abweichend zur [SICCT] das Kommando „SICCT SELECT CT MODE" der SICCT-Spezifikation NICHT unterstützen.
[<=]

Das eHealth-Kartenterminal antwortet bei nicht unterstützten Kommandos (dazu zählen neben SICCT SELECT CT MODE auch die optionalen Kommandos SICCT COMFORT ENROLL und SICCT COMFORT AUTH bei Nichtumsetzung) gemäß [SICCT#5.4.2] mit 6D00 (Wrong instruction). Einzige Ausnahme bildet das Kommando SICCT CONTROL, auf das gemäß [TIP1-A_3264] mit 6200 geantwortet werden muss.

3.7.11 Einschränkung des Command-To-Perform Data Objects

TIP1-A_3013 - Einschränkungen CMD DO
Das eHealth-Kartenterminal DARF einschränkend zu Kapitel "5.5.10.23 Command-To-Perform Data Object" der SICCT-Spezifikation im Command-To-Perform Data Object CMD DO im Control Byte andere Werte als {b2=1, b1=0} oder {b2=1, b1=1} NICHT unterstützen.
[<=]

3.8 Verhalten bei der PIN-Eingabe

TIP1-A_3090 - PIN mit variabler oder fixer Länge
Das eHealth-Kartenterminal MUSS unabhängig davon, ob es sich um eine Eingabe von einer PIN mit variabler oder fixer Länge handelt, die Bestätigung der Eingabe der PIN durch Drücken einer „Enter"-Taste (dies legt nicht die Beschriftung dieser Taste, sondern lediglich ihre Funktion bei der PIN-Eingabe fest) implementieren.
[<=]

Dieses ergänzt die Funktionsbeschreibung von Abschnitt 5.19 der SICCT-Spezifikation [SICCT] wie auch andere Spezifikationsabschnitte, die eine PIN-Eingabe erfordern.

TIP1-A_3091 - PIN-Länge Kartenterminal bekannt
Das eHealth-Kartenterminal DARF bei bekannter PIN-Länge (entweder von einer Applikation übergeben oder durch das PIN-Format vorgegeben) und falls diese unterschritten wird, die "Enter"-Taste NICHT akzeptieren.
[<=]

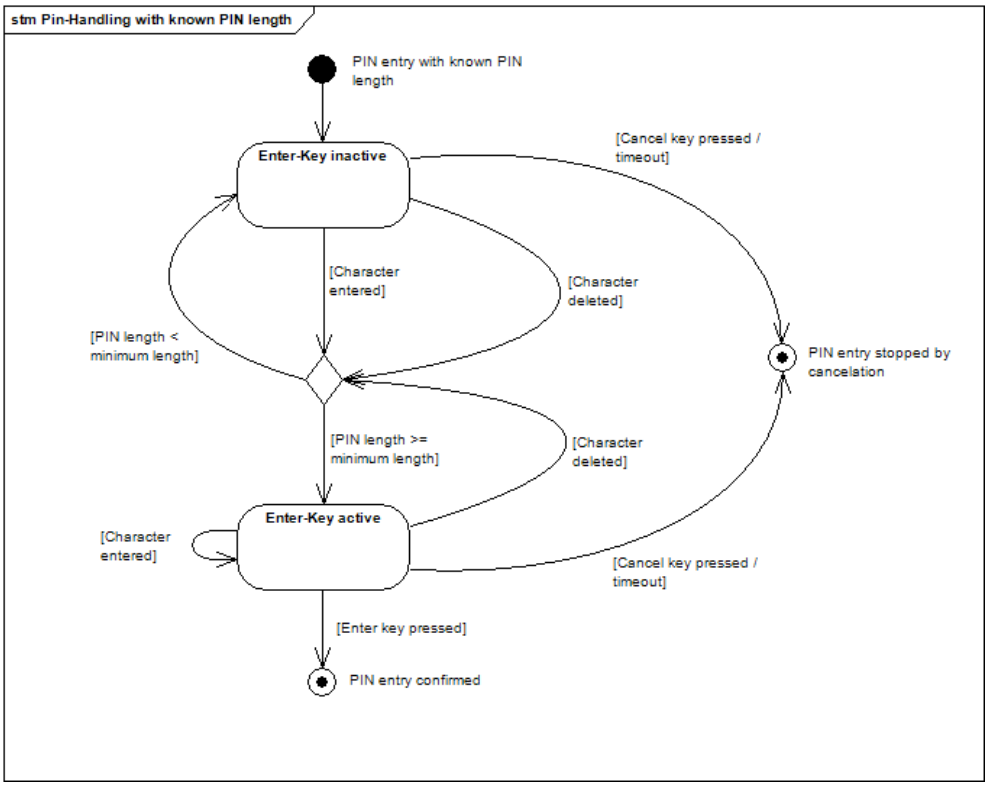


Abbildung 11: Pic_KT_0014 Verhalten bei PIN-Eingabe mit bekannter Länge

Die folgenden Anforderungen gelten insbesondere für solche Kartenterminals, deren Display lediglich die minimalen Anforderungen von zwei Zeilen zu je 16 Zeichen erfüllen.

TIP1-A_3132 - Anzahl der während der PIN-Eingabe anzeigbaren Zeichen
Das eHealth-Kartenterminal DARF die Länge der eingebbaren PIN NICHT über die Anzahl der während der PIN-Eingabe anzeigbaren Zeichen begrenzen.
[<=]

Das bedeutet, wenn auch nur noch sechs Zeichen für eine Anzeige der PIN-Eingabe (16 Zeichen Maximalbreite – 10 Zeichen PIN-Prompt=6 Zeichen) zur Verfügung stehen, darf allein dadurch die maximale Länge einer PIN durch das Kartenterminal nicht auf diese sechs Zeichen begrenzt werden.

TIP1-A_3133 - PIN-Länge mindestens 12 Zeichen ermöglichen
Das eHealth-Kartenterminal MUSS grundsätzlich die Eingabe von PINs mit einer PIN-Länge von mindestens 12 Zeichen ermöglichen.
[<=]

TIP1-A_3134 - Während der PIN-Eingabe
Das eHealth-Kartenterminal MUSS während der PIN-Eingabe den Fortgang der Eingabe für den Benutzer erkennbar anzeigen.
[<=]

TIP1-A_3135 - Anzahl eingegebene Zeichen
Das eHealth-Kartenterminal MUSS für den Benutzer während der PIN-Eingabe jederzeit erkennbar anzeigen, wie viele Zeichen er bereits eingegeben hat.
[<=]

Als Lösung wäre denkbar, dass bereits angezeigte Ersatzzeichen nach links verschoben werden, auch wenn dadurch der PIN-Prompt sukzessive überschrieben wird. Es ist auch vorstellbar, dass im Display die jeweilige Stelle der PIN-Eingabe in Form einer Nummer angegeben wird. Die genauen Details zur Umsetzung sind herstellerspezifisch.

3.9 Festlegungen zur Sicherung der Firmware Updates

TIP1-A_3092 - Aktualisierung der Kartenterminal-Firmware
Das eHealth-Kartenterminal MUSS sicherstellen, dass die Aktualisierung der eHealth-Kartenterminal-Firmware mittels asymmetrischer kryptographischer Verfahren geschützt wird.
[<=]

Konkret wird nur eine Sicherung der Authentizität und Integrität gewährleistet. Dies ist durch eine Signatur durch den Terminalhersteller zu gewährleisten. Die Signatur durch den Kartenterminalhersteller 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. Das Format der Firmware (d. h. des Binärfiles) bleibt herstellerspezifisch.

TIP1-A_3108 - Prüfung der einzuspielenden Firmware-Version
Das eHealth-Kartenterminal MUSS die Prüfung einer einzuspielenden Firmware-Version stets durch die zu diesem Zeitpunkt auf dem eHealth-Kartenterminal aktive Firmware durchführen.
[<=]

TIP1-A_3093 - Neu einzuspielende Firmware-Version
Das eHealth-Kartenterminal MUSS die zur Prüfung einer neu einzuspielenden Firmware-Version erforderlichen öffentlichen Schlüssel für die Signaturprüfung in der aktiven Firmware enthalten.
[<=]

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 Signatur-Envelope ein- bzw. angefügt wird.

3.10 Auswahl kryptographischer Algorithmen für TLS

Für die Transportverschlüsselung mittels TLS für die SICCT-spezifische TLS-Verbindung und die Netzwerk-basierten Managementschnittstellen müssen die in [gemSpec_Krypt#5.9] angegebenen Cipher Suites verpflichtend, wie in [gemSpec_Krypt#A_17089] und [gemSpec_Krypt#A_17090] definiert, unterstützt werden.

3.11 Authentisierung beim Aufbau der SICCT-spezifischen TLS-Verbindungen

TIP1-A_3253 - Kommunikation gemäß SICCT-Protokoll
Das eHealth-Kartenterminal MUSS für den Aufbau der nach [SICCT] spezifizierten SICCT-spezifischen TLS-Verbindung, die zur Nutzung für eine Kommunikation gemäß SICCT-Protokoll vorgesehen ist, ausschließlich eine gegenseitige Authentisierung zwischen Server (Kartenterminal) und Client (Konnektor) implementieren.
Präsentiert der Client (Konnektor) beim TLS-Verbindungsaufbau kein Zertifikat, MUSS das eHealth-Kartenterminal SICCT- bzw. EHEALTH-Kommandos, die nicht in [gemSpec_KT#CMD_KT_0004] angeführt sind, ablehnen.
[<=]

Andere Authentisierungsverfahren (einseitige Authentifizierung, Whitelist etc.) zum Aufbau der SICCT-spezifischen TLS-Verbindung sind nicht zulässig. Diese Anforderungen gelten nicht für den Aufbau administrativer TLS-Verbindungen, wie z. B. HTTPS-Verbindungen, welche rein zur Administration oder Konfiguration des Terminals bestimmt sind (siehe 2.4.5).

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 und gepairtes Kartenterminal ist. Die Betriebszulassung 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.

TIP1-A_3254 - Prüfung betriebszugelassener Konnektor
Das eHealth-Kartenterminal MUSS bei der Authentisierung gemäß [TIP1-A_3253] überprüfen, ob es sich um einen betriebszugelassenen Konnektor handelt.
[<=]

Der Ablauf des TLS-Verbindungsaufbaus zwischen einem TLS-Client und dem Kartenterminal ist im folgenden Diagramm „Pic_KT_0016 TLS-Verbindungsaufbau“ informativ dargestellt.

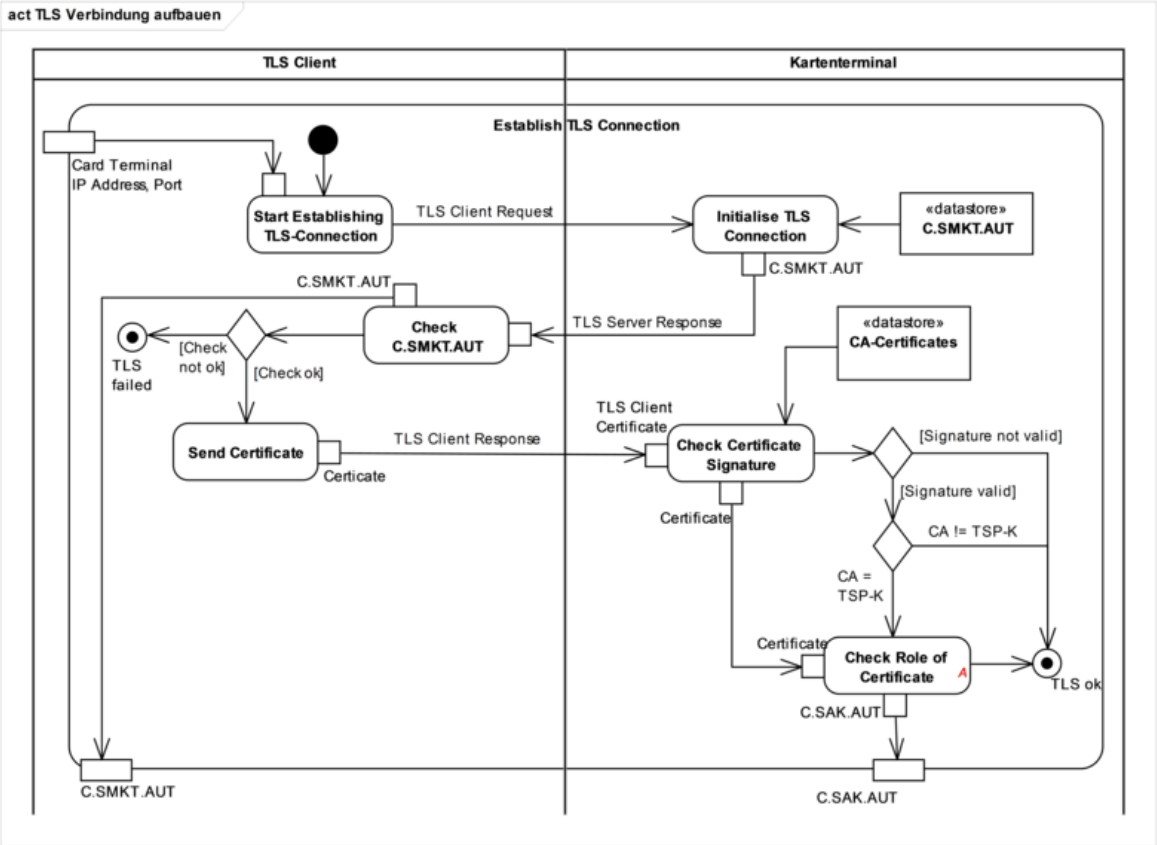


Abbildung 12: Pic_KT_0016 TLS-Verbindungsaufbau

Komponentenzertifikate für Konnektoren werden durch Trusted Service Provider für Komponentenzertifikate (TSP) ausgestellt. Jedes Komponentenzertifikat eines Konnektors kann auf ein CA-Zertifikat innerhalb der Trust-service Status List (TSL) zurückgeführt werden.

TIP1-A_3255 - CA-Zertifikate der relevanten TSP speichern
Das eHealth-Kartenterminal MUSS mindestens die CA-Zertifikate der TSP aus der integeren und authentischen TSL speichern (z. B. in der Firmware), die Komponentenzertifikate für einen Konnektor erzeugen.
[<=]

Die Dienste bzw. CA-Zertifikate in der TSL sind über die TSL-Extension zuordenbar: Im Extensioneintrag wird zu jedem CA-Zertifikat angegeben, welche Typen von Zertifikaten er ausstellen darf (siehe [gemSpec_TSL#7.3.2.1]). Ein Filtern nach relevanten TSPs ist damit einfach möglich.

TIP1-A_3256 - CA-Zertifikate in Kartenterminal und anschließende Speicherung
Das eHealth-Kartenterminal MUSS beim Einbringen von CA-Zertifikaten in das Kartenterminal und ihrer anschließenden Speicherung innerhalb des Kartenterminals deren Authentizität gewährleisten.
[<=]

TIP1-A_3257 - Schutz CA-Zertifikate
Das eHealth-Kartenterminal MUSS gespeicherte CA-Zertifikate gegen Veränderungen schützen.
[<=]

TIP1-A_6482 - Anzahl CA-Zertifikate
Das eHealth-Kartenterminal MUSS zu einem Zeitpunkt mindestens zehn CA-Zertifikate pro Vertrauensraum speichern können.
[<=]

Wenn zeitgleich mehrere verschiedene Vertrauensräume in der Firmware des eHealth-Kartenterminals hinterlegt sind, so ist die Anzahl entsprechend zu vervielfachen.

TIP1-A_3094 - Aktualisierung von CA-Zertifikaten der Komponenten-PKI
Nehmen neue CAs ihren Betrieb für das Generieren von Komponentenzertifikaten für Konnektoren auf, MUSS das eHealth-Kartenterminal die zugehörigen CA-Zertifikate auf vertrauenswürdige Weise übernehmen.
[<=]

TIP1-A_3158 - TSP-Update-Mechanismus
Hersteller KÖNNEN zur Umsetzung von [TIP1-A_3094] einen TSP-Update-Mechanismus am eHealth-Kartenterminal implementieren, welcher es ermöglicht, die Liste der TSP CAs auszutauschen.
[<=]

TIP1-A_3159 - TSP-Update-Mechanismus für KT ohne Firmware-Update
Ein eHealth-Kartenterminal, das den TSP-Update-Mechanismus gemäß [TIP1-A_3158] umsetzt, DARF für diesen ein Firmware-Update NICHT nutzen bzw. erforderlich machen.
[<=]

Die Sicherheit des TSP-Update-Mechanismus ist im Rahmen der Common Criteria Evaluierung nachzuweisen. Die Details zur Umsetzung sind herstellerspezifisch.

TIP1-A_3941 - Update von TSP-Zertifikaten
Der Hersteller eines eHealth-Kartenterminals KANN zur Umsetzung von [TIP1-A_3094] das Update von TSP-Zertifikaten über ein Update der Firmware des Kartenterminals realisieren.
[<=]

TIP1-A_3940 - Zertifikat prüfen
Das eHealth-Kartenterminal MUSS, zur Feststellung gemäß [TIP1-A_3254], ob das ansteuernde System ein betriebszugelassener Konnektor ist, das vom Konnektor präsentierte Zertifikat prüfen.
[<=]

Dabei können Teile des Use Cases TUC_PKI_018 [gemSpec_PKI#8.3.1.1] verwendet werden, wobei die einzelnen Schritte jedoch an die Gegebenheiten des Kartenterminals angepasst werden müssen. Für die Verifikation müssen die folgenden Punkte umgesetzt werden.

Für eine automatische Prüfung der Betriebszulassung eines Konnektors durch andere IT-Systeme steht ein X.509-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.

TIP1-A_3933 - Mathematische Prüfung Zertifikat
Das eHealth-Kartenterminal MUSS das beim TLS-Aufbau präsentierte Konnektorzertifikat entsprechend TUC_PKI_004 gemäß [gemSpec_PKI#8.3.1.4] prüfen.
[<=]

TIP1-A_3934 - Ermittlung Zertifikatsrolle
Das eHealth-Kartenterminal MUSS aus dem beim TLS-Aufbau präsentierten Konnektorzertifikat entsprechend TUC_PKI_009 gemäß [gemSpec_PKI#8.3.3.2] die Rolle ermitteln.
[<=]

TIP1-A_3935 - Vergleich Zertifikatsrolle
Das eHealth-Kartenterminal MUSS überprüfen, dass die in [TIP1-A_3934] ermittelte Rolle der Rolle "Signaturanwendungskomponente (SAK)" (oid_sak gemäß gemSpec_OID#3.5.4) entspricht.
[<=]

TIP1-A_4115 - Sicherstellung CA Berechtigung
Im Rahmen der Prüfung nach [TIP1-A_3933] MUSS das eHealth-Kartenterminal sicherstellen, dass nur Zertifikate von CAs zur Prüfung herangezogen werden, die berechtigt sind, Konnektorzertifikate auszustellen.
[<=]

Die folgende Tabelle zeigt die einzelnen Schritte, die durchgeführt werden müssen:

Tabelle 16: Schritte beim Verifizieren des Zertifikats einer Signaturanwendungskomponente (SAK)

Aufgabe	TUC gemäß [gemSpec_PKI]	Besonderheit
Gültigkeit des Zertifikats prüfen	-	Wird nicht durchgeführt. Siehe Anmerkungen unten.
CA-Zertifikat der ausstellenden CA suchen	-	Muss anhand der gespeicherten CA-Zertifikate durchgeführt werden. Siehe Anmerkungen unten.
Prüfung der Signatur über das Zertifikat	TUC_PKI_004	-
Prüfung, ob CA Zertifikate für Konnektoren ausstellen darf	-	Wird organisatorisch im Vorfeld oder technisch geregelt. Siehe Anmerkungen unten.
Ermittlung der Rolle des Zertifikats	TUC_PKI_009	Ausgabe: OID der Rolle
Abgleich der Rolle mit der technischen Rolle "Signaturanwendungskomponente (SAK)"	-	OID = oid_sak?

Anmerkungen:

- Ein eHealth-Kartenterminal verfügt über keine Systemuhr und keine Datumsangaben. Es kann daher die Gültigkeit des Komponentenzertifikats nicht überprüfen.
- Es muss die Liste der in dem eHealth-Kartenterminal intern gespeicherten CA-Zertifikate durchsucht werden (siehe [TIP1-A_3936]). Zu einem

Komponentenzertifikat eines Konnektors erfüllt (nur) das korrekte CA-Zertifikat folgende Bedingungen (siehe auch TUC_PKI_003 in [gemSpec_PKI#8.3.1.3]):

issuerDN Komponentenzertifikat = subjectDN CA-Zertifikat

authorityKeyIdentifier Komponentenzertifikat = subjetKeyIdentifier CA-Zertifikat

- Wird [TIP1-A_4115] nicht technisch im Kartenterminal umgesetzt, dann muss durch organisatorische Maßnahmen sichergestellt werden, dass nur für solche CAs die CA-Zertifikate in das eHealth-Kartenterminal eingebracht werden, die auch tatsächlich Komponentenzertifikate für Konnektoren ausstellen dürfen (siehe [TIP1-A_3937]).

TIP1-A_3936 - Durchsuchen CA-Zertifikate
Das eHealth-Kartenterminal MUSS für die Prüfung gemäß [TIP1-A_3933] die Liste der im eHealth-Kartenterminal gespeicherten CA-Zertifikate durchsuchen.
[<=]

TIP1-A_3937 - Einbringen CA-Zertifikate
Der Hersteller des eHealth-Kartenterminals MUSS im Fall, dass [TIP-A_4115] nicht technisch im Kartenterminal umgesetzt wird, durch organisatorische Maßnahmen sicherstellen, dass nur für solche CAs die CA-Zertifikate in das eHealth-Kartenterminal eingebracht werden, die auch tatsächlich Komponentenzertifikate für Konnektoren ausstellen dürfen.
[<=]

Das Komponentenzertifikat des Konnektors wird durch das eHealth-Kartenterminal nur dann akzeptiert, falls alle Schritte ohne Fehler durchgeführt werden können.

TIP1-A_3095 - Aufbau des SICCT-spezifischen TLS-Kanals bei nicht-gültigem Konnektorzertifikat
Das eHealth-Kartenterminal MUSS unabhängig davon, ob es sich beim während des Aufbaus des SICCT-spezifischen TLS-Kanals vom Client präsentierten Zertifikat um ein gültiges Konnektorzertifikat handelt oder nicht, den Verbindungsaufbau akzeptieren.
[<=]

TIP1-A_3136 - Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei ungültigem Konnektorzertifikat
Das eHealth-Kartenterminal DARF im Fall, dass es sich beim während des Aufbaus des SICCT-spezifischen TLS-Kanals vom Client präsentierten Zertifikat nicht um ein gültiges Konnektorzertifikat handelt, SICCT- bzw. EHEALTH-Kommandos, die nicht in [gemSpec_KT#CMD_KT_0004] angeführt sind, NICHT ausführen.
[<=]

TIP1-A_3096 - Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei gültigem Konnektorzertifikat ohne Pairing
Das eHealth-Kartenterminal DARF im Fall, dass es sich beim während des Aufbaus des SICCT-spezifischen TLS-Kanals vom Client präsentierten Zertifikat um ein gültiges Konnektorzertifikat handelt, das Kartenterminal jedoch nicht über Pairing-Informationen verfügt oder der öffentliche Schlüssel des präsentierten Zertifikats nicht in diesen enthalten ist, es SICCT- bzw. EHEALTH-Kommandos, die nicht in [gemSpec_KT#CMD_KT_0004] oder [gemSpec_KT#CMD_KT_0005] angeführt sind, NICHT ausführen.
[<=]

TIP1-A_3097 - Aufbau des SICCT-spezifischen TLS-Kanals, erlaubte Kommandos bei gültigem Konnektorzertifikat mit Pairing
Das eHealth-Kartenterminal MUSS alle SICCT- und EHEALTH-Befehle dieses Clients akzeptieren, wenn der öffentliche Schlüssel des beim Verbindungsaufbaus vom Client präsentierten Zertifikats in einem Pairing-Block enthalten ist und es sich beim während des Aufbaus des SICCT-spezifischen TLS-Kanals vom Client präsentierten Zertifikat um ein gültiges Konnektorzertifikat handelt.
[<=]

TIP1-A_3266 - Kartenkommandos ablehnen bei nicht vorhandenem Pairing
Das eHealth-Kartenterminal DARF ISO-7816 APDUs für eine Chipkarte (siehe SICCT#6.1.4.2 wSrcOrDesAddr) NICHT akzeptieren, wenn der öffentliche Schlüssel des beim Verbindungsaufbaus vom Client präsentierten Zertifikats nicht in einem Pairing-Block enthalten ist und es sich beim während des Aufbaus des SICCT-spezifischen TLS-Kanals vom Client präsentierten Zertifikat nicht um ein gültiges Konnektorzertifikat handelt.
[<=]

In dieser Phase wird das korrekte Shared Secret (ShS.KT.AUT) nur durch den Konnektor geprüft. (Durch einen folgenden Aufruf von EHEALH TERMINAL AUTHENTICATE mit P2=02 gemäß Abschnitt 2.5.2.2). 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, 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 3.11.2 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 Pairing-Information vorhanden, so prüft der Konnektor nach erfolgtem TLS-Aufbau die Pairing-Information (siehe Kapitel 2.5.2.2). Schlägt diese Prüfung fehl, wird die Verbindung abgebrochen.

3.11.1 Positivliste für Kommandos ohne gültiges Konnektorzertifikat

Unabhängig vom Stand des Pairings (siehe dazu Kap. 2.5.2) und unabhängig vom während des TLS-Verbindungsaufbaus vom Client präsentierten Zertifikat muss es am Kartenterminal möglich sein, ein Firmware Update zu ermöglichen und Statusinformationen abzufragen.

TIP1-A_3137 - „Liste ausführbarer Kommandos ohne gültiges Konnektorzertifikat“
Das eHealth-Kartenterminal MUSS nach dem TLS-Verbindungsaufbau unabhängig vom Stand des Pairings und unabhängig vom während des TLS-Verbindungsaufbaus vom Client präsentierten Zertifikats am Kartenterminal die in [gemSpec_KT#CMD_KT_0004] „Liste ausführbarer Kommandos ohne gültiges Konnektor-zertifikat" gelisteten Kommandos ausführen können.
[<=]

Andere SICCT- oder EHEALTH-Kommandos als die in Tabelle 18 gelisteten Kommandos dürfen nicht ausgeführt werden, falls es sich bei dem zum TLS-Verbindungsaufbau präsentierten Clientzertifikat um kein gültiges Konnektorzertifikat handelt (siehe [TIP1-A_3136]).

Tabelle 17: Liste ausführbarer Kommandos ohne gültiges Konnektorzertifikat (CMD_KT_0004)

Kommandobezeichner
SICCT CT INIT CT SESSION
SICCT CT CLOSE CT SESSION
SICCT GET STATUS
SICCT SET STATUS
SICCT CT DOWNLOAD INIT
SICCT CT DOWNLOAD DATA
SICCT CT DOWNLOAD FINISH

3.11.2 Positivliste für Kommandos ohne gültige Pairing-Information

Unabhängig vom Stand des Pairings (siehe dazu Kap. 2.5.2) und unabhängig vom während des TLS-Verbindungsaufbaus vom Client präsentierten Zertifikat muss es möglich sein, das Kartenterminal in Betrieb zu nehmen.

TIP1-A_3098 - Aufbau des SICCT-spezifischen TLS-Kanals, zusätzlich erlaubtes Kommando bei gültigem Konnektorzertifikat ohne Pairing
Das eHealth-Kartenterminal MUSS zusätzlich zu den in [gemSpec_KT#CMD_KT_0004] gelisteten Kommandos auch die in [gemSpec_KT#CMD_KT_0005] gelisteten Kommandos unabhängig vom Stand des Pairings am Kartenterminal zur Ausführung anbieten, wenn es sich beim während des Aufbaus des SICCT-spezifischen TLS-Kanals vom Client präsentierten Zertifikat um ein gültiges Konnektorzertifikat handelt.
[<=]

Andere SICCT- oder EHEALTH-Kommandos als jene in Tabelle 19 sowie in Tabelle 18 (siehe Kapitel 3.11.1) aufgeführten dürfen nicht ausgeführt werden, falls der öffentliche Schlüssel des beim TLS-Verbindungsaufbau präsentierten Konnektorzertifikats nicht in den Pairing-Informationen des Kartenterminals enthalten ist (siehe [TIP1-A_3096]).

Tabelle 18: Liste ausführbarer Kommandos ohne gültige Pairing-Information (CMD_KT_0005)

Kommandobezeichner
EHEALTH TERMINAL AUTHENTICATE

3.12 Abbau der SICCT-spezifischen TLS-Verbindung

TIP1-A_3258 - Beendigung SICCT-spezifische TLS-Verbindung, resetten der Karten
Das eHealth-Kartenterminal MUSS, wenn die nach [SICCT] spezifizierte SICCT-spezifische TLS-Verbindung, die zur Nutzung für eine Kommunikation gemäß SICCT-Protokoll vorgesehen ist, beendet wird, alle in ihm gesteckten Karten inkl. eventuell vorhandener SMCs resetten.
[<=]

TIP1-A_3259 - Beendigung SICCT-spezifische TLS-Verbindung, Verlust der Sicherheitszustände
Das eHealth-Kartenterminal MUSS, wenn die nach [SICCT] spezifizierte SICCT-spezifische TLS-Verbindung, die zur Nutzung für eine Kommunikation gemäß SICCT-Protokoll vorgesehen ist, beendet wird, eventuell erlangte Sicherheitszustände verlieren.
[<=]

3.13 Auslieferungszustand

TIP1-A_3099 - Auslieferungszustand Kennwörter
Das eHealth-Kartenterminal MUSS im Auslieferungszustand leere/ungesetzte Kennwörter aufweisen.
[<=]

TIP1-A_3100 - Auslieferungszustand Pairing-Information
Das eHealth-Kartenterminal MUSS im Auslieferungszustand leere bzw. ungesetzte Pairing-Informationen aufweisen.
[<=]

TIP1-A_3101 - Auslieferungszustand Managementschnittstelle
Das eHealth-Kartenterminal MUSS im Auslieferungszustand alle Managementschnittstellen des Kartenterminals deaktiviert haben.
[<=]

TIP1-A_3102 - Auslieferungszustand Direktkennwort
Das eHealth-Kartenterminal MUSS im Auslieferungszustand sicherstellen, dass die einzige erlaubte Funktion am Kartenterminal das Setzen des Direktkennwortes ist.
[<=]

TIP1-A_3103 - Erstmaliges Setzen des Direktkennworts
Das eHealth-Kartenterminal MUSS bis zum erstmaligen Setzen des Direktkennworts die lokalen Anschlüsse und den SICCT-Port deaktiviert haben.
[<=]

Dies gilt ergänzend zu den Festlegungen zum Auslieferungszustand in Abschnitt 6.1.5 der SICCT-Spezifikation („Auslieferungszustand“).

Die sich hieraus ergebenden Konfigurationsschritte eines Kartenterminals sind im nachfolgenden Diagramm „Pic_KT_0015 Inbetriebnahme“ dargestellt.

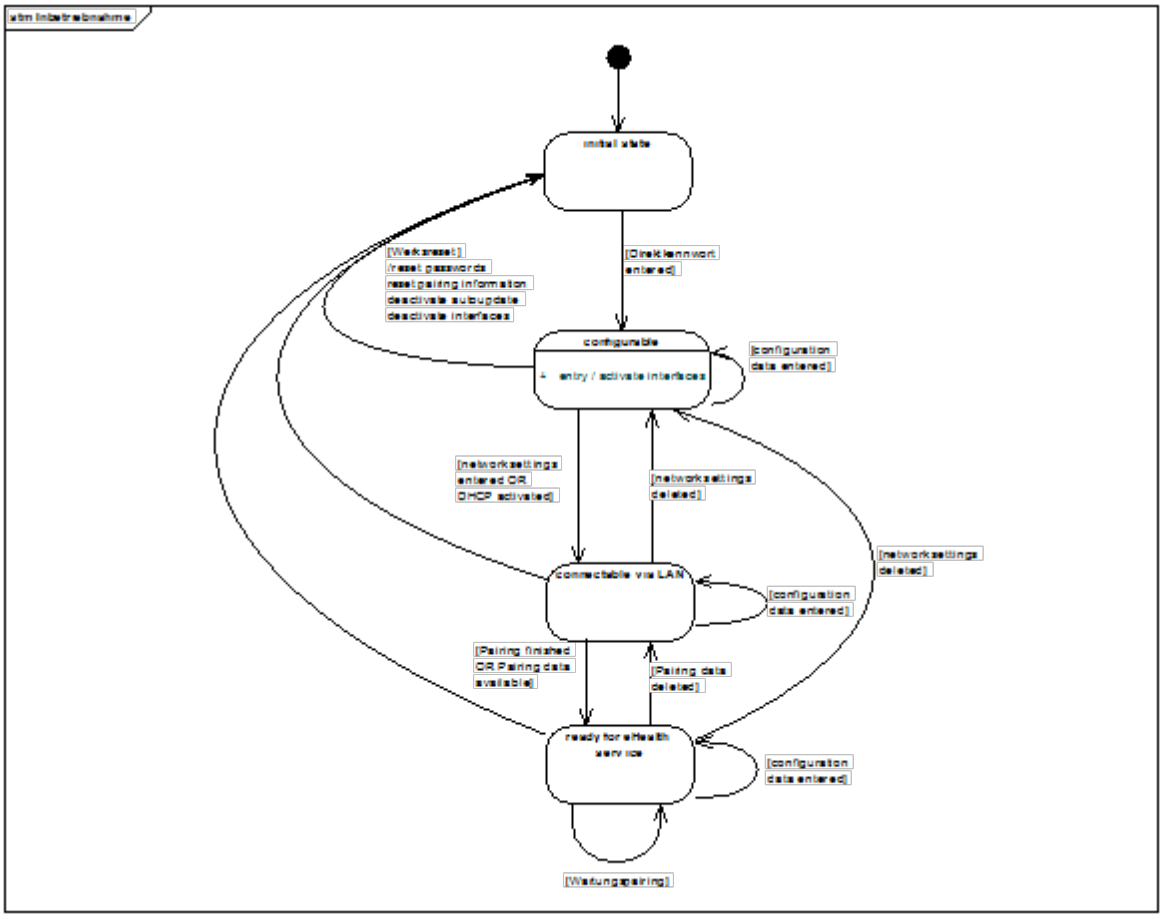


Abbildung 13: Pic_KT_0015 Inbetriebnahme

Nach dem Setzen des Direktkennwortes ist eine Einbringung des Kartenterminals in das in der dezentralen Umgebung installierte Netz möglich.

Für den Fall, dass das Kartenterminal die Netzwerkskonfigurationsdaten nicht dynamisch erhält, muss eine statische Konfiguration über eine Managementschnittstelle erfolgen.

Im nächsten Schritt ist das initiale Pairing durchzuführen (siehe Kapitel 2.5.2.1).

Danach ist das Kartenterminal in der Lage, seinen Service mit einem Konnektor auszuführen.

In jedem Zustand ist die Konfiguration des Kartenterminals änderbar sowie ein Werksreset durchführbar (siehe Abschnitt 3.14).

3.14 Werksreset

TIP1-A_3417 - Möglichkeit zum Werksreset
Das eHealth-Kartenterminal MUSS über eine Möglichkeit zum Werksreset verfügen.
[<=]

TIP1-A_3104 - Definition Werksreset
Das eHealth-Kartenterminal MUSS die Konfigurationen durch einen Werksreset in den Auslieferungszustand zurücksetzen, jedoch nicht die Firmware und die Firmwaregruppe.
[<=]

Siehe Abbildung „Pic_KT_0015 Inbetriebnahme“. Die Firmware selbst ist in diesem Zusammenhang nicht zu betrachten.

TIP1-A_3424 - Werksreset Administrator
Das eHealth-Kartenterminal MUSS die Möglichkeit zum Werksreset gemäß [TIP1-A_3417] ausschließlich dem Administrator zur Verfügung stellen.
[<=]

TIP1-A_3420 - Weiterer Mechanismus für Werksreset
Der Hersteller des eHealth-Kartenterminals MUSS für den Werksreset neben [TIP1-A_3424] einen weiteren Mechanismus zur Durchführung anbieten, welcher die Arbeitsabläufe beim Leistungserbringer bzw. in der Organisation des Gesundheitswesens nur minimal unterbricht.
[<=]

Die minimale Unterbrechung ist wie folgt definiert: Ein eHealth-Kartenterminal muss dem Leistungserbringer bzw. dem Mitarbeiter der Organisation des Gesundheitswesens zur Verfügung stehen. Eine Konfiguration eines eHealth-Kartenterminals ist jedoch nicht vermeidbar.

TIP1-A_3154 - Authentisierung für weiteren Werksreset-Mechanismus
Das eHealth-Kartenterminal MUSS sicherstellen, dass der Mechanismus gemäß [TIP1-A_3420] ausschließlich nach Authentisierung durch eine Kombination aus Username und Passwort oder einen mindestens gleich starken Mechanismus ausgeführt werden kann.
[<=]

TIP1-A_3421 - PUK-Verfahren
Das eHealth-Kartenterminal KANN zur Umsetzung von [TIP1-A_3420] ein PUK-Verfahren implementieren, bei welchem über eine Managementschnittstelle eine PUK zur Durchführung eines Werksresets gesetzt werden kann.
[<=]

TIP1-A_3425 - Dokumentation Werksreset Mechanismus
Der Hersteller des eHealth-Kartenterminals MUSS die Umsetzung von [TIP1-A_3420] in der Benutzerdokumentation beschreiben und die aus Sicht des Anwenders notwendigen Schritte verständlich darstellen.
[<=]

TIP1-A_5424 - Ausführung eines Werksreset ohne Authentisierung
Der Hersteller des eHealth-Kartenterminals KANN einen zusätzlichen Werksreset-Mechanismus ohne vorherige Authentisierung implementieren (d.h. der Werksreset ist von jeder Person ausführbar).
[<=]

TIP1-A_5425 - Aktivierung/Deaktivierung des Werksreset ohne Authentisierung
Falls der zusätzliche Werksreset-Mechanismus ohne Authentisierung gemäß [TIP1-A_5424] implementiert wird, MUSS das eHealth-Kartenterminal ausschließlich dem Administrator die Aktivierung und Deaktivierung dieses Mechanismus ermöglichen.
[<=]

TIP1-A_5426 - Standardeinstellung Werksreset ohne Authentisierung
Falls der zusätzliche Werksreset-Mechanismus ohne Authentisierung gemäß [TIP1-A_5424] implementiert wird, MUSS das eHealth-Kartenterminal diesen Mechanismus als Standardeinstellung deaktivieren.
[<=]

Wenn der Werksreset-Mechanismus ohne vorherige Authentisierung implementiert und aktiviert ist, kann der Anwender im Einzelfall wählen, welchen der Werksreset-Mechanismen (authorisiert oder unauthorisiert) er ausführen möchte.

TIP1-A_3418 - Werksreset nicht dauerhaft unausführbar
Das eHealth-Kartenterminal DARF durch einen Werksreset bei sachgemäßer Handhabung und ohne technisches Versagen NICHT einen Zustand einnehmen, der einen erneuten Werksreset unausführbar macht. Der Auslieferungszustand für das Direktkennwort gemäß [TIP1-A_3102] sowie ggf. die PUK-Eingabe bei Inbetriebnahme gemäß [TIP1-A_3422] bleiben hiervon unberührt.
[<=]

Die Umsetzung des Werksreset-Mechanismus ist herstellerspezifisch.

4 Anhang A - Verzeichnisse

4.1 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	Heilberufsausweis, 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
SMKT-Identität	Security Modul Kartenterminal-Identität
TSL	Trust-service Status List
TSP	Trusted Service Provider
TLS	Transport Layer Security

TCP/IP	Transmission Control Protocol over Internet Protocol
VerSA	Verteilte Signatur Arbeitsplätze
ZLS	Zulassungsschlüssel
ZOD	Zahnärzte Online Deutschland

4.2 Glossar

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

4.3 Tabellenverzeichnis

Tabelle 1: Tab_KT_003 Anforderungen Klima 22
Tabelle 2: Tab_KT_004 Anforderungen Vibration 22
Tabelle 3: Tab_KT_005 Karten-Kompatibilität....47
Tabelle 4: Kommandosequenz EHEALTH TERMINAL AUTHENTICATE CREATE ‘P2=01’ (SEQ_KT_0001) 57
Tabelle 5: Kommandosequenz EHEALTH TERMINAL AUTHENTICATE ADD Phase 1 ‘P2=03’ (SEQ_KT_0003) 61
Tabelle 6: Kommandosequenz EHEALTH TERMINAL AUTHENTICATE ADD Phase 2 ‘P2=04’ (SEQ_KT_0004) 64
Tabelle 7: Command Definition EHEALTH TERMINAL AUTHENTICATE (CMD_KT_0001)....66
Tabelle 8: EHEALTH AUTHENTICATE Response Structure Definition (CMD_KT_0002) 69
Tabelle 9: EHEALTH AUTHENTICATE Status Code Definition (CMD_KT_0003)....69
Tabelle 10: Shared Secret Data Object Definition (DO_KT_0003) 70
Tabelle 11: Shared Secret Challenge Data Object Definition (DO_KT_0004) 71
Tabelle 12: Shared Secret Response Data Object Definition (DO_KT_0005) 71
Tabelle 13: Discretionary Data Data Object Definition (DO_KT_0001)....74
Tabelle 14: Discretionary Data Data Object Type Definition (DO_KT_0002)....75
Tabelle 15: Sicherheitsprotokolle (DO_KT_0006) 76
Tabelle 16: Schritte beim Verifizieren des Zertifikats einer Signaturanwendungskomponente (SAK) 83
Tabelle 17: Liste ausführbarer Kommandos ohne gültiges Konnektorzertifikat (CMD_KT_0004)....86
Tabelle 18: Liste ausführbarer Kommandos ohne gültige Pairing-Information (CMD_KT_0005)....86

4.4 Abbildungsverzeichnis

Abbildung 1: Pic_KT_0004 Physische Ausprägung Kartenterminal....9
Abbildung 2: Pic_KT_0006 Schnittstellen des Kartenterminals....10
Abbildung 3: PIC_KT_0001 – gematik-Prüfzeichen....17
Abbildung 4: Pic_KT_0007 Initiales Pairing Schritt 2....42
Abbildung 5: Pic_KT_0008 Wartungs-Pairing....45
Abbildung 6: Pic_KT_0009 EHEALTH AUTHTENTICATE CREATE....56
Abbildung 7: Pic_KT_0010 EHEALTH AUTHTENTICATE VALIDATE....59
Abbildung 8: Pic_KT_0011 EHEALTH AUTHENTICATE - ADD Phase 1....61
Abbildung 9: Pic_KT_0012 EHEALTH AUTHENTICATE - ADD Phase 2....63
Abbildung 10: Pic_KT_0013 Zustandsdiagramm EHEALTH EXPECT CHALLENGE RESPONSE....65
Abbildung 11: Pic_KT_0014 Verhalten bei PIN-Eingabe mit bekannter Länge....78
Abbildung 12: Pic_KT_0016 TLS-Verbindungsaufbau....81
Abbildung 13: Pic_KT_0015 Inbetriebnahme....88

4.5 Referenzierte Dokumente

4.5.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert; Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellen, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[eGK]	Generation 1 / 1plus: ~~[gemSpec_eGK_P1]:~~ ~~gematik: Die Spezifikation elektronische Gesundheitskarte ;~~ ~~Teil 1 – Spezifikation der elektrischen Schnittstelle~~ ~~[gemSpec_eGK_P2]~~ ~~gematik: Die Spezifikation elektronische Gesundheitskarte ;~~ ~~Teil 2 – Grundlegende Applikationen~~ Generation 2/2.1: [gemSpec_COS] gematik: Spezifikation COS Spezifikation der elektrischen Schnittstelle [gemSpec_eGK_ObjSys] gematik: Spezifikation der elektronischen Gesundheitskarte eGK-Objektsystem [gemSpec_eGK_OPT] gematik: Spezifikation der elektronischen Gesundheitskarte Äußere Gestaltung
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemSpec_Kon]	gematik: Konnektorspezifikation
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_KSR]	gematik: Spezifikation Konfigurationsdienst
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_OM]	gematik: Übergreifende Spezifikation Operations und Maintenance
[gemSpec_PKI]	gematik: Übergreifende Spezifikation PKI
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemSpec_Perf]	gematik: Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform
[gemZul_KT]	gematik: Verfahrensbeschreibung Zulassung von dezentalen IT-Komponenten in der Telematikinfrastruktur (Stationäres Kartenterminal)

[gSMC-KT]	[gemSpec_COS] gematik: Spezifikation COS Spezifikation der elektrischen Schnittstelle [gemSpec_gSMC-KT_ObjSys] gematik: Spezifikation gSMC-KT-Objektsystem
[HBA]	[gemSpec_COS] gematik: Spezifikation COS Spezifikation der elektrischen Schnittstelle [gemSpec_HBA_ObjSys] gematik: Spezifikation HBA Objektsystem
[HBA-qSig]	BÄK (2009): Zertifikatsprofile für X.509-Attributzertifikate, V2.3.1 http://www.bundesaerztekammer.de/page.asp?his=1.134.3421.4132
[SMC-B]	[gemSpec_COS] gematik: Spezifikation COS Spezifikation der elektrischen Schnittstelle [gemSpec_SMC-B_ObjSys] gematik: Spezifikation SMC-B Objektsystem
[ZOD]	KZBV Telematik (2011): ZOD 2.0 – Anforderungsprofil für ZOD-Anbieter http://www.kzbv.de/rahmenrichtlinien-fuer-anbieter.158.de.html

4.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI-M2.11]	BSI: IT-Grundschutzkataloge – Maßnahmenkatalog Organisation (15. Ergänzungslieferung 2016) https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf
[BSI-CC-PP-0032]	BSI: Common Criteria Protection Profile – Electronic Health Card Terminal (eHCT), BSI-CC-PP-0032
[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
[DAHZ]	DAHZ Hygieneleitfaden Ausgabe 7 (2006): Hygieneleitfaden des Deutschen Arbeitskreises für Hygiene in der Zahnmedizin

[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
[ISO14443-P1]	ISO/IEC 14443-1 (15.4.2000): Identification cards – Contactless integrated circuit(s) cards – Proximity cards - Part 1: Physical characteristics
[ISO14443-P2]	ISO/IEC 14443-2 (1.6.2001): Identification cards – Contactless integrated circuit(s) cards – Proximity cards - Part 2: Radio frequency power and signal interface
[ISO14443-P3]	ISO/IEC 14443-3 (1.2.2001): Identification cards – Contactless integrated circuit(s) cards – Proximity cards - Part 3: Initialization and anticollision
[ISO14443-P4]	ISO/IEC 14443-4 (1.2.2000): Identification cards – Contactless integrated circuit(s) cards – Proximity cards - Part 4: Transmission protocol
[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
[ISO7816-3]	ISO/IEC 7816-3 (2006): Identification cards – Integrated circuit(s) cards with contacts Part 3 – Electronic signals and transmission protocols
[KVK]	Technische Spezifikation der Versichertenkarte, 2009, Version: 2.08
[RFC2119]	RFC 2119 (March1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt
[RFC2246]	RFC 2246 (Januar 1999): The TLS Protocol, Version http://www.ietf.org/rfc/rfc2246.txt
[RFC3927]	RFC 3927 (Mai 2005) Dynamic Configuration of IPv4 Link-Local Addresses http://www.ieft.org/rfc/rfc3927.txt

[RFC4346]	RFC 4346 (April 2006): The Transport Layer Security (TLS) Protocol Version 1.1 http://www.ietf.org/rfc/rfc4346.txt
[RFC5246]	RFC 5246 (August 2008): The Transport Layer Security (TLS) Protocol Version 1.2; http://tools.ietf.org/html/rfc5246
[RFC 5746]	RFC 5746 (February 2010) Transport Layer Security (TLS) Renegotiation Indication Extension http://tools.ietf.org/html/rfc5746
[RKI]	Robert-Koch-Institut (2004): Anforderungen an die Hygiene bei der Reinigung und Desinfektion von Flächen – Empfehlung der Kommission für Krankenhaushygiene und Infektionsprävention beim Robert-Koch-Institut (RKI)
[SICCT]	SICCT (17.12.2010): TeleTrusT, SICCT Secure Interoperable ChipCard Terminal, Version 1.21
[TR-03115]	BSI (19.10.2007): Komfortsignatur mit dem Heilberufsausweis
[TR-03120]	BSI (23.10.2007): TR-3120 Technische Richtlinie zur Kartenterminalidentität Version 1.0
[TR-03120-Anhang]	BSI (04.04.2008): Anhang zur Technischen Richtlinie BSI TR-03120 Version 1.0.2
[TRBA 250]	Ausschuss für Biologische Arbeitsstoffe – ABAS: Technischen Regeln für Biologische Arbeitsstoffe im Gesundheitswesen und in der Wohlfahrtspflege Ausgabe: November 2003 Änderung und Ergänzung Juli 2006 (Bundesarbeitsblatt 7-2006, S. 193) Ergänzung April 2007, GMBl Nr. 35 v. 27. Juli 2007, S. 720 Änderung und Ergänzung November 2007, GMBl Nr.4 v. 14.02.2008, S. 83
PRODSG	BGBl. I S. 2179; 2012 I S. 131 (2011): Gesetz über die Bereitstellung von Produkten auf dem Markt (Produktsicherheitsgesetz - ProdSG)