Bundesamt
für Sicherheit in der
Informationstechnik

BSI - Technische Richtlinie

Bezeichnung:	**Sichere Kartenterminalidentität (Betriebskonzept)**
Anwendungsbereich:	eHealth Kartenterminals
Kürzel:	BSI TR-03120
Version:	1.0
Veröffentlichung:	23.10.2007

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-111
E-Mail: zertifzierung@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhalt

Vorwort

Das Leben im 21. Jahrhundert wird immer mehr von der Informations- und Kommunikationstechnik geprägt.
Digitale Prozesse ersetzen nicht nur Papierlösungen sondern tragen auch wesentlich dazu bei, sichere und schnelle Methoden zur Identifikation und Authentifikation zu schaffen.

Die elektronische Gesundheitskarte (eGK) und der Heilberufsausweis (HBA) sind Beispiele dieser neuen Prozesse, die ohne Medienbrüche zu einer schnellen und zuverlässigen Patientenverwaltung und insbesondere der papierlosen elektronischen Rezepterstellung beitragen sollen.

Hierzu werden hohe Anforderungen an Funktionalität und Sicherheit an die eingesetzten Komponenten gestellt.
Zum Schutz der Information, zur Wahrung der Vertraulichkeit, der Integrität und der Verfügbarkeit müssen sichere IT-Produkte eingesetzt werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet bereits seit vielen Jahren Informationen und Hilfestellungen rund um das Thema IT-Sicherheit.

Diese Technische Richtlinie dient mit einem praktischen Betriebskonzept als Empfehlung bei der Etablierung einer eindeutigen Terminalidentifikation in einem Netzwerk als Basis für eine authentische und gesicherte Kommunikation.

Einführung

Speziell im deutschen Gesundheitswesen sollen mehrere Kartenterminals in einem Netzwerk mit einem Host (hier Konnektor) vertraulich kommunizieren.
Dabei soll gleichzeitig gewährleistet werden, dass die eindeutige Zuordnung des Kartenterminals sichergestellt wird und der Konnektor somit nur mit dem vorbestimmten, authentischen Kartenterminal kommuniziert.
Ein Netzwerk kann nicht in allen Fällen physisch abgesichert sein, da es sich über Raum- und Gebäudegrenzen hinaus erstrecken kann.
Zum Schutz der Anwendung sind Maßnahmen erforderlich, die eine gesicherte und authentische Kommunikation zwischen den Kommunikationspartnern Kartenterminal und (ansteuerndem) Konnektor gewährleisten.
Diese benötigen eine eindeutige Identität abgebildet durch, Zertifikate und Geheimnisse.
Die Wahrung der Identität muss auch nach einer Veränderung der Firmware durch Upgrades/Fehlerkorrekturen und ohne Audit des gesamten Firmware Source Codes gewährleistet sein.

Ziel

Globale Anforderungen an Sicherheitsziele der eHealth Anwendung sind neben dem Schutz der digitalen Signatur des Heilberufsausweises vor unautorisierter Nutzung und dem Schutz der Daten der eGK gegen Ausspähung auch der Schutz der Infrastruktur gegen unautorisierte Inbetriebnahme von Komponenten.

Weitere Sicherheitsziele, insbesondere im Kontext der digitalen Signatur, erfordern eine umfangreichere Betrachtung und sind nicht Gegenstand dieser Dokumentation.

Ziel ist es, ein Verfahren zu beschreiben, bei dem es möglich ist, eine vertrauenswürdige Zuordnung (authentische Identität), sowie eine abhörsichere (vertrauliche) und manipulationssichere (integere) Verbindung zwischen Kartenterminal und Konnektor herzustellen.

Hierbei werden die Schutzmechanismen der Chipkartenbetriebssysteme gegen Angriffe auf die Daten einer Chipkarte als Stand der Technik vorausgesetzt und hier nicht weiter betrachtet.

Allgemeine Anforderungen, die durch das Signaturgesetz (SigG) bzw. der Signaturverordnung (SigV) bedingt sind (z. B. sichere PIN-Eingabe), werden ebenfalls an dieser Stelle nicht betrachtet.

Das in dieser TR beschriebene Verfahren beruht auf Methoden, die durch vorangegangenen Spezifikationen der SICCT-Terminalhersteller [Auth06] und des BMG/BSI [WP1.6] abgestimmt und untersucht worden sind.

Es werden nur Sicherheitsaspekte eines Terminals gegenüber dem Konnektor betrachtet. Das gilt sowohl für Terminals am Netzwerk direkt als auch für Terminals, die über den Proxy eines PCs verbunden sind.

Für eine eindeutige Identität werden kryptographische Verfahren verwendet, die ein Zertifikat mit privaten Schlüsseln in einem sicheren Schlüsselspeicher nutzen.

Bei diesem Verfahrene wird als sicherer Schlüsselspeicher eine Chipkarte oftmals in Form einer SMC (ID-000, Plug-in Chipkarte) realisiert. Dieser spezielle Typ einer SMC wird SM-KT genannt.

Eine SM-KT stellt eine Sonderform einer SMC-A dar. Mittels einer Kennzeichnung im Attributszertifikat wird der Unterschied verdeutlicht.

Wenn organisatorische und sicherheitstechnische Belange zufrieden stellend dargelegt werden können und sofern auch die damit verbundenen funktionellen Prozesse voneinander unbeeinflusst sind, dann könnten die Daten der SM-KT auch in die Hardware der SMC-A oder SMC-B integriert werden.

Da jedoch noch ungeklärte Fragen zur Prozesstrennung bei der Personalisierung, zum sicheren Auslieferungsprozess, der Aufbewahrung und des Betriebs existieren wird in den folgenden Ausführungen eine getrennte SM-KT in Form einer sicherheitsevaluierten Prozessorchipkarte angenommen.

Damit kann auf bereits zertifizierte Komponenten und etablierte Standardprozesse für Produktion und Distribution dieser Komponente zurückgegriffen werden.

Das im Folgenden beschriebene Betriebskonzept geht von einer nicht automatischen Inbetriebnahme durch Unterstützung eines Administrator des Konnektors oder eines geschulten Servicepersonals aus. Damit können auch große Installationen mit vielen Terminals von einer zentralen Stelle aus administriert werden.

1. Referenzen

[Auth06] SICCT
Authentisierung und Schlüsselmanagement für SICCT eHealth Terminals V1.01, 19.09.2006

[WP1.6] Whitepaper BMG/BSI
Betriebskonzept zur Nutzung der SM-KT zur eindeutigen kryptographisch gesicherten Kommunikation, V1.6, 01.06.2007

2. Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
EAL	Evaluation Assurance Level
ICC	Integrated Circuit Card
IT	Informationstechnik
KT	Kartenterminal
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
QES	Qualifizierte Elektronische Signatur
SigG	Signaturgesetz
SigV	Signaturverordnung
SMC	Secure Module Card
SM	Secure Module
SSL	secure socket layer
SICCT	Secure Interoperable Chipcard Terminal
TCP/IP	Transmission Control Protocol over Internet Protocol
TLS	Transport Layer Security
TR	Technische Richtlinie

3. Sicherheitsziele

S01.) Schutz der Kommunikation gegen Datenmanipulation
S02.) Schutz der Kommunikation vor Ausspähen
S03.) Schutz vor Vortäuschung einer falschen Identität des Kommunikationspartners

4. Bedrohung

B01.) Mitlesen der Kommunikation zwischen Kartenterminal und Konnektor.
B02.) Angriff auf eine Kommunikation durch Unterschieben nicht autorisierter Daten.
B03.) Umlenkung der Kommunikation über einen unautorisierten Dritten (man in the middle).
B04.) Nutzung eines manipulierten Terminals.
B05.) Unautorisierte Erzeugung einer Terminalidentität.
B06.) Diebstahl der Terminalidentität und Nutzung in einem anderen Kartenterminal.
B07.) Diebstahl eines Terminals und Wiedereinbringung mit kompromittierter Funktion.
B08.) Unautorisierte Anmeldung eines Kartenterminals am Konnektor.

5. Generische Maßnahmen

M01.) Als Schutz vor Datenmanipulation wird Authentisierungsfunktion einer SSL/TLS Verbindung zwischen Kartenterminal und Konnektor genutzt.

M02.) Als Schutz vor Ausspähen von Daten wird die Verschlüsselungseigenschaft einer SSL/TLS Verbindung genutzt.

M03.) Als Schutz vor Vortäuschung einer falschen Identität des Kommunikationspartners wird eine fälschungssichere kryptographische Identität verwendet.

M04.) Als Schutz der Firmware und Daten im Kartenterminal wird das Gehäuse in geeigneter Form versiegelt.

M05.) Als Schutz vor Manipulation an der SM-KT wird der zugriffsgesicherte sicherheitsevaluierte Speicher einer Prozessorkarte genutzt.

M06.) Als Schutz vor Diebstahl und/oder irregulären Verwendung der SM-KT wird die SM-KT durch einen Pairingprozess logisch mit dem Kartenterminal gekoppelt.

6. Annahmen

[A1] Die Inbetriebnahme bzw. der Einsatz des Kartenterminals erfolgt generell in einer kontrollierten Umgebung.

[A2] Die Inbetriebnahme des Terminals und damit die Schaffung der Identität erfolgt in einer durch den Administrator überwachten Umgebung.

[A3] Der Betrieb des Kartenterminals erfolgt über eine ansteuernde Instanz (Konnektor).

[A4] Das Kartenterminal verfügt über die Möglichkeit zur Transportsicherung auf Basis SSL/TLS.

[A5] Das Kartenterminal kann so konfiguriert werden, dass nur (SSL) gesicherte Kommunikationen möglich sind.

[A6] Kartenterminal und Konnektor bilden einen kryptographisch gesicherten Kanal.

[A7] Die Sicherheit des sicheren Kanals beruht auf dem Austausch beglaubigter Zertifikate. Die Beglaubigung kann durch einen Administrator nach Prüfung der Sicherheitskriterien wie Authentizität des Gerätes und Unversehrtheit der Sicherheitssiegel erfolgen.

[A8] Das Kartenterminal verfügt eine einmalige interne und gleichzeitig von außen sichtbare MAC-Adresse.

[A9] Die SM-KT verfügt über eine sichtbar aufgebrachte einmalige Identifikationsnummer oder einen Fingerprint des öffentlichen Schlüssels.

[A10] Es wird eine einmalige Kartenterminalidentität genutzt.

[A11] Kartenterminal, SM-KT und Konnektor werden gepaart, so dass die Kartenterminalidentität an die Hardwarekombination Kartenterminal+SM-KT gebunden ist.

[A12] Für den Aufbau der TLS Verbindung werden sowohl auf Konnektorseite als auch auf Terminalseite X509 Zertifikate benötigt. Es wird davon ausgegangen, dass die verwendeten Schlüssellängen nach einigen Jahren als unsicher eingestuft werden und die Gerätezertifikate ersetzt werden müssen.

[A13] Das Kartenterminal gibt bestimmte Daten nur über eine kryptographisch gesicherte Verbindung heraus.

[A14] Der Nutzer und Administrator kontrollieren die Unversehrtheit des Kartenterminals.

7. Sicherheitsmechanismen

1. Verschlüsselung der Kommunikation zwischen Kartenterminal und Konnektor.
2. Authentisierung des Terminals durch den Konnektor durch Nutzung einer SM-KT.
3. Authentische Kommunikation zwischen Kartenterminal und Konnektor (beidseitige Authentisierung mit Überprüfung des Zertifikates bzw. der Root.
4. Versiegelung des Kartenterminal -Gehäuses
5. Erzeugung eines Kartenterminal-individuellen Authentisierungsdatensatzes im Konnektor aus SM-KT Identität und Terminalkennung die individuell, nicht vorhersagbar und eindeutig ist.
6. Authentisierungsdaten bestehen aus einer kryptografischen Identität in der SM-KT und einmaligen Daten der beteiligten Komponenten.
7. Aufbau einer TLS Verbindung zur verschlüsselten Übertragung der Authentisierungsdaten.
8. Inbetriebnahme/ Initialisierung des Terminals am Konnektor erfolgt durch einen Administrator.
9. Die Initialisierung eines Terminals mit Hilfe des Konnektors erfolgt in einer überschaubar sicheren räumlichen Umgebung. So ist z.B. administrativ sicher zustellen, dass in dieser Zeit kein Publikumsverkehr in der räumlichen Umgebung der Initialisierung stattfindet.
10. Abmeldung (Deregistrierung) defekter oder entwendeter Terminals im Konnektor durch einen Administrator.
11. Automatisches Abmelden des Terminals im Konnektor bei fehlerhafter Terminalidentität mit Notwendigkeit der Neuanmeldung und eines administratorgestützten Pairingprozesses.

8. Betriebskonzept

8.1 Basis

Für die kryptografische Identität wird eine Chipkarte (vorzugsweise im ID-000 Format) verwendet.

Zwar kann mit Hilfe des Zertifikates in der SM-KT eine TLS verschlüsselte Verbindung zum Konnektor aufgebaut werden, jedoch ist das Zertifikat zunächst keinem bestimmten Kartenterminal zugeordnet. Das SM-KT wird erst durch einen Paarungsprozess (Pairing) logisch mit der Hard- und Software des Kartenterminals verbunden.

Eine einzelne SM-KT oder auch eine entwendete SM-KT ist daher nicht brauchbar.

Zudem kann die SM-KT beim Endnutzer vor Ort in einem Inbetriebnahmeprozess von einem Administrator eingebracht werden.

Die Einbringung der SM-KT durch einen Administrator bei Aufstellung der Kartenterminals ist sicherer und praktikabler als eine Einbringung beim Hersteller weil:

- es keinen unkontrollierten Verbleib von Terminalidentitäten im Warenversand und Service gibt,
- die Identität bei Defektgeräten oder Reparaturaustausch entnommen und in der Obhut des Administrators verbleiben kann,
- die SM-KT bei unzureichender Schlüssellänge gegen eine neue ausgetauscht werden kann (Nutzungsdauer des Terminals übersteigt die durch den Algorithmenkatalog zugelassene Nutzungsdauer der Algorithmen bei angewandten Schlüssellängen)
- Es können die etablierten Vertriebsstrukturen der SMC verwendet werden.

8.2 Inbetriebnahme

Mit der Anlieferung der Kartenterminals bei den Leistungserbringern erfolgt der Übergang der Verantwortung auf die Leistungserbringer.
Der Leistungserbringer selbst oder ein von ihm beauftragter Administrator führt die Inbetriebnahme der vom Hersteller versiegelten Geräte durch.

Über etablierte Vertriebswege werden die SM-KT vom Administrator beschafft. Die SM-KT enthalten X.509 Zertifikate, die von einer Root signiert wurden und die von den Konnektoren geprüft werden können. Zusätzlich ist auf der SM-KT ein Fingerprint (zum public key) aufgedruckt oder es existiert eine direkt mit individuellen Merkmalen der SM-KT verbundene Verknüpfung zu einem Fingerprint.

Der Administrator muss durch Augenschein, Prüfung der Transportsiegel und Lieferinformationen den Originalzustand eines gelieferten Terminals beurteilen und nur Geräte die der Beschreibung des Herstellers entsprechen und mit unversehrten Siegeln versehen sind in Betrieb nehmen.

Wichtig ist bei allen Verfahren, dass das Siegel vom Administrator bei der Initialisierung und auch vom Endnutzer (Heilberufler) bei der ersten Nutzung, unter Verwendung aller Sicherheitsmerkmale (s. Annahmen, Kapitel 6), auf Unversehrtheit überprüft wird, um kein manipuliertes Kartenterminal am Konnektor anzumelden, bzw. die Anwendung mit einem manipulierten Kartenterminal zu beginnen.

1. Der Administrator steckt das SM-KT ins Kartenterminal (bzw. verschieden SM-KTs in mehrere Terminals), notiert sich die (aufgedruckte und angezeigte) MAC-Adresse des Kartenterminals und ordnet den Fingerprint des eingesteckten SM-KT dem jeweiligen Kartenterminal/MAC-Adresse zu.
2. Der Administrator startet die Kartenterminalverwaltung am Konnektor.
3. Der Konnektor zeigt die MAC-Adressen aller im Netz befindlicher Kartenterminals an
4. Der Administrator wählt nun die MAC Adresse des (ersten) Kartenterminals aus.
5. Der Konnektor baut eine TLS Vermindung zum ausgewählten Kartenterminal auf und erhält dabei das Zertifikat (aus der SM-KT) welches er in Bezug auf die Root überprüft.
6. Der Konnektor zeigt dem Administrator den Fingerprint des erhaltenen Zertifikats (public keys) an.
7. Damit die SM-KT nur in genau dem einen KT verwendet werden kann, ist eine weitere Kopplung zwischen KT und SM-KT erforderlich (Pairing).
8. Der eigentliche Pairingprozess beginnt, indem der Administrator den korrekten Fingerprint bestätigt.
9. Zunächst wird mittels eines speziellen Pairingkommandos vom Konnektor eine 16 Byte lange Terminalkennung erzeugt und zusammen mit einer Displaymeldung über die TLS gesicherte Verbindung an das Kartenterminal gesendet.
10. Der Administrator MUSS den Abschluss dieses halbautomatischen Pairingprozesses am Kartenterminals nach Überprüfung des authentischen Gerätezustands und der Displaymessage auslösen.
11. Vor der Speicherung der Terminalkennung im geschützten Bereich des Kartenterminals führt das Terminal eine Zertifikatsprüfung gegenüber der Konnektor-Root durch
12. In der Antwort auf das Pairingkommando wird die von der SM-KT signierte Terminalkennung an den Konnektor zurückgesendet.
13. Der Konnektor kann mit dieser Antwort abschließend noch kontrollieren ob die Terminalkennung der zugeordneten Kombination aus MAC-Adresse und SM-KT entspricht.
14. Weitere Terminals können gleichartig, beginnend mit Schritt 3. angemeldet werden.

Die vom Konnektor generierte Terminalkennung verhindert eine Nutzung der SM-KT in einem anderen, möglicherweise modifizierten Kartenterminal.

Kartenterminal und SM-KT sind damit logisch verbunden.

Wenn die SM-KT entnommen (entwendet) wird und eine neue SM-KT eingesetzt wird, ist ein erneutes Pairing erforderlich.

Ein neues (halbautomatisches) Pairing mit der gleichen SM-KT kann erst durch eine Administratorhandlung am Konnektor erfolgen.

8.3 Betrieb

Nach jedem neuen Aufbau einer SSL/TLS Session, wird die Kartenterminalidentität vom Konnektor abgefragt und mit den gespeicherten Informationen verglichen.

Wenn der Vergleich negativ ausfällt wird eine weitere Kommunikation zum Kartenterminal unterbunden. Im Konnektor wird das Ereignis protokolliert und dem Administrator die Empfehlung einer Neuinitialisierung angezeigt.

Dazu werden individuelle und zufällige Daten verwendet.

Es wird hierzu vom Konnektor mittels eines speziellen Kartenterminalkommandos eine Zufallszahl an das Kartenterminal gesendet. Das Kartenterminal antwortet mit der von der SM-KT signierten Kombination aus Terminalkennung und gesendeten Zufallszahl.

Der Konnektor überprüft, dass es sich nicht um ein Replay-Angriff handelt (aktuelle Zufallszahl) und verifiziert die korrekte Terminalkennung.

Sollte dem Nutzer eine Unregelmäßigkeit am Kartenterminal auffallen, so ist die Unversehrtheit des Gehäuses zu überprüfen. Es darf kein neuer Pairingprozess vom Nutzer ohne einer Interaktion mit dem Konnektor vorgenommen werden.

Wenn der Konnektor keine eindeutige Zuordnung zum Kartenterminal vornehmen kann, muss ein neuer Pairingprozess angestoßen werden. Hierzu sind alle Maßnahmen bzw. Vorkehrungen aus dem Prozess der Inbetriebnahme anzuwenden.

9. Abwehr der Bedrohungen

Das Mitlesen der Kommunikation zwischen Kartenterminal und Konnektor wird durch eine TLS/SSL Verbindung verhindert.

Auch der Angriff auf eine Kommunikation durch Unterschieben nicht autorisierter Daten und ein „man in the middle“ Angriff wird durch die Etablierung eines authentischen und kryptographisch gesicherten Kanals unterbunden.

Ein manipuliertes Terminal wird durch Veränderungen am Gehäuse oder an Veränderungen an den Sicherheitssiegeln erkennbar.

Eine unautorisierte Erzeugung einer Terminalidentität wird durch den aktiven Einsatz eines Administrators mit Zugriffsrechten am Konnektor verhindert.

Der Diebstahl der Terminalidentität und die Nutzung in einem anderen Kartenterminal werden durch die SM-KT und das Pairing (Erzeugen und Nutzung einer Terminalkennung) verhindert.

Der Angreifer kann die SM-KT aus den Kartenterminal stehlen. Dann fehlt ihm immer noch die Terminalkennung.

Der Angreifer kann das ganze Kartenterminal stehlen - das fällt auf und ein Nutzer oder Administrator wird das Kartenterminal dann aus der Liste im Konnektor austragen.

Eine befristete Entwendung über Nacht wird aufgrund der „kontrollierten Einsatzumgebung“ verhindert (Zutrittsschutz). Sollten Zweifel bestehen, so ist vor der Erstverwendung (am Morgen) die Unversehrtheit des Gehäuses genau zu überprüfen.

Sollte versucht werden, ein Kartenterminal auszutauschen, so ist neben dem Besitz der SM-KT zusätzlich noch die Kenntnis der generierten Terminalkennung erforderlich. Das erfordert einen mehrstündigen Zugriff auf das auszutauschende Kartenterminals und ein aufwändiges „Reverse-Engineering“ der Kartenterminalsoftware.

Ein Einlöten des Sicherheitsmoduls oder ähnliche mechanische Maßnahmen ist daher nicht gesondert notwendig.

Ein „Reverse-Engineering“ ist zudem aufwändiger als ein Auslöten oder Aussägen des Sicherheitsmoduls.

Der Angreifer könnte versuchen, einen Konnektor im Netzwerk zu simulieren um in den Besitz der Daten (Terminalkennung) zur Terminalidentität zu gelangen.

Da er die SSL/TLS Verbindung zum Kartenterminal nicht aufbauen kann, können die Informationen nicht gelesen werden.

Zudem verhindert die Verschlüsselung mit dem Public Key des (rechtmäßigen) Konnektors die Kenntnisnahme der Daten.

Wenn es dem Angreifer gelingt die Kommunikationsleitung des SM-KT mitzuschneiden, kann er trotzdem die SSL Session nicht abhören, da der SSL Sessionkey aus zwei Komponenten besteht von denen nur eine über das SM-KT verschlüsselt wird. Der Angreifer ist also weiterhin gezwungen das Kartenterminal selbst zu manipulieren.

Auch die Terminalkennung ist nicht abgreifbar da sie verschlüsselt übertragen wird.

Der Zugriff über die Schnittstellen des Kartenterminals auf den Flash Speicher (externer Zugriff) ist nicht möglich. Der Inhalt des Flash Speichers ist ohne Verletzung der Gehäusesiegel nicht auslesbar.

Eine nachträgliche Rückentwicklung (Reverse-Engineering) zur Ermittlung der Terminalkennung würde eine nahezu vollständige Rückentwicklung des Betriebssystems des Terminals erfordern und ist damit äußerst aufwändig. Der erlangte Schlüssel würde auch nur die Identität eines einzelnen Kartenterminals an einem bestimmten Konnektor kompromittieren und ist daher nur von begrenzter Tragweite.

Jeder Versuch auf die im Kartenterminal beständig (persistent) gespeicherten Informationen zuzugreifen ist mit einer sichtbaren Zerstörung der Gehäusesiegel verbunden. Auch eine durch Reverse-Engineering gewonnene Information muss in ein zweites bzw. manipuliertes KT eingebracht werden, bei dem die Manipulation ebenfalls durch eine fehlende oder nicht ordnungsgemäße Versiegelung festgestellt werden kann.

Der in dieser TR beschriebene Prozess gilt für den Einsatz eines Terminals in einer kontrollierten Umgebung.

Bei Terminals in nicht kontrollierten Umgebungen kann durch gesonderte Maßnahmen eine Löschung der beständigen Daten bei einem Sabotageversuch unternommen werden, so dass der pure Besitz der SM-KT nutzlos ist.

Vorteile dieses Verfahrens sind, dass

- die Übertragung der Terminalkennung ist unbeobachtbar und zwangsläufig nur zwischen dem vom Administrator ausgewählten Kartenterminal und administrierten Konnektor möglich,
- der Administrator durch Augenschein, Prüfung der Transportsiegel und Lieferinformationen den Originalzustand eines gelieferten Terminals beurteilen kann und nur unverdächtige Geräte in Betrieb nimmt,
- ein aus einer Praxis gestohlenes Gerät durch die Terminalkennung nur am gleichen Konnektor als authentisch bekannt ist und kann daher in keiner anderen Anwendungsumgebung für einen Angriff genutzt werden kann,
- gestohlene Geräte aus der Whitelist eines Konnektors gelöscht werden, so dass ein "Wiederauftauchen" in (kompromittierter) Form wirkungslos ist,
- fabrikneue Geräte können ebenfalls nicht ins System eingeschleust werden können, da kein (passendes) SM-KT vorhanden ist,

- der Administrationszugang zu einem Konnektor abgesichert ist, wodurch unerwünschte Authentisierungen verhindert werden,
- die Terminalkennung ist an Kartenterminal, MAC-Adresse und SM-KT gebunden ist und damit ein "Transplantat" sofort erkannt wird,
- die sicherheitssensitive SM-KT nicht allein ausreicht, was die Anforderungen an Überwachung, Protokollierung und Vertriebswege für SM-KTs reduziert,
- das Verfahren keine Kosten für zusätzliche Hardware erfordert,
- das vorgestellte Verfahren durchaus vergleichbar mit dem Einbuchen von schnurlosen Telefonen, Bluetooth Komponenten oder einer WLAN Schlüsseleingabe ist und damit vielen Administratoren durchaus geläufig ist,
- keine aufwändigen Bedienvorgänge am Kartenterminal nötig sind, nachdem das SM-KT eingebracht worden ist.

Die Rolle des Administrators gibt es in der Konnektor- und auch in der SICCT Spezifikation. Bei jeder Inbetriebnahme sind Eingaben am Kartenterminal und auch am Konnektor nötig, wie z. B. Friendly Names und Workplace ID. Die zusätzliche Initialisierung der Terminalkennung ist kein großer Mehraufwand und kann nach Bestätigung durch den Administrator halbautomatisch erfolgen.

Durch organisatorische Vorgaben kann erreicht werden, dass entwendete Geräte im Konnektor gelöscht werden.

Anzuwendende Mechanismen:

M01.) Verschlüsseln der Kommunikation mittels SSL/TLS Transportsicherung.
M02.) Zertifikatsbasierte Authentifikation (X.509-Zertifikate).
M03.) Nutzung individueller Schlüssel (TLS Sessionkey pro Kartenterminal).
M04.) Erzeugung der Terminalidentität mit Hilfe des Konnektors.
M05.) Pairing der SM-KT mit dem Terminal und damit Untrennbarkeit.
M06.) TLS Verbindung zwischen Kartenterminal und Konnektor mittels des mit der SM-KT gespeicherten Zertifikates und kryptografischen Geheimnisses.
M07.) Einbringung des Terminalidentität in das Kartenterminal über die verschlüsselte SSL Verbindung.
M08.) Nutzung einer Terminalkennung und der MAC-Adresse.
M09.) Authentisierung mittels der Terminalidentität (Terminalkennung+ SM-KT) zu Beginn jeder TLS Session.
M10.) Versiegelung des Terminals mittels vom BSI zertifizierter Siegel.

Die (geeignete) Versiegelung des Kartenterminals ist daher ein elementares Element bei der sicheren Nutzung des Flash Speichers und der Terminal-Firmware.

Ein Angriff erfordert das Brechen der Siegel des Terminals mit nachfolgendem Reverse-Engineering zur Erlangung der Terminalkennung. Um die gewonnene Information zu nutzen, muss daraufhin der Angreifer ein kompromittiertes Kartenterminal in die Ursprungsumgebung einbringen und darauf hoffen dass das zeitweise Fehlen des Gerätes und die gebrochenen Siegel nicht auffallen.

Unter diesen Voraussetzungen wäre vermutlich eine Nutzung des manipulierten Betriebssystems direkt zur Informationsgewinnung lohnender und ein Angriff auf die Authentisierungsinformationen nicht mehr nötig.

Das Terminal ist CC / EAL3+ evaluiert und besitzt ausreichende Mechanismen zum Schutz der internen Komponenten (Betriebssystem, interne Speicher).

Wenn mit gleichem Aufwand (Reverse-Engineering) für die Überwindung der Terminalauthentisierung gleichzeitig weiterreichende Angriffsmöglichkeiten eröffnet werden, so wird die Terminalauthentisierung nicht mehr primär das Ziel des Angreifers.