Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03119

Anforderungen an Chipkartenleser mit nPA Unterstützung

Version 1.2

27. Mai 2011

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: ePA@bsi.bund.de
Internet: https://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

Inhalt

Tabellenverzeichnis

Abbildungsverzeichnis

Version	*Datum*	*Änderungen*
1.1	15.12.09	Version 1.1 der Technischen Richtlinie
1.2	27.05.11	Grundlegende Überarbeitung, Fehlerkorrekturen, Berücksichtigung praktischer Erfahrungen

1 Einleitung

Der neue Personalausweis (nPA) vereint den herkömmlichen Ausweis und drei neue elektronische Funktionen im Scheckkartenformat:

- Gegenseitiger elektronischer Identitätsnachweis (eID-Funktion) für E-Business- und E-Government-Anwendungen
- Qualifizierte elektronische Signatur (QES-Funktion) nach deutschem Signaturgesetz für E-Business- und E-Government-Anwendungen
- Elektronische Identitätsfeststellung ausschließlich durch hoheitliche Anwendungen

Die Daten werden auf einem in die Chipkarte integrierten RF-Chip gespeichert. Die Kommunikation zwischen dem Chip und einem kontaktlosen Chipkartenleser erfolgt über induktive Kopplung nach ISO 14443.

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

Mit dieser Technischen Richtlinie soll eine Basis geschaffen werden, die untereinander kompatible Chipkartenleser erwirkt, die zudem in möglichst vielen weiteren Anwendungen eingesetzt werden können. Auch soll es hiermit Anwendungsentwicklern ermöglicht werden, auf eine einheitliche Schnittstelle aufsetzen zu können, um so zur Technischen Richtlinie konforme Chipkartenleser beliebiger Hersteller verwenden zu können.

Die wichtigste Anforderung an einen Chipkartenleser ist der fehlerfreie, störungsfreie und zuverlässige Betrieb sowie die Unversehrtheit der Chipkarten. Dazu sind bei kontaktlosen und kontaktbehafteten Chipkartenlesern weitere Anforderungen und Funktionen zur Sicherstellung der Interoperabilität notwendig. Ebenso muss die Informationssicherheit berücksichtigt werden, um die Vertraulichkeit und die Integrität der Abläufe und der Kommunikation gewährleisten zu können.

Zwar gibt es beim neuen Personalausweis (nPA) eine direkte Verwandtschaft zum elektronischen Reisepass (ePass), jedoch erfordern zum Beispiel qualifizierte elektronische Signaturen (QES) und geplante nicht-hoheitliche Anwendungen besondere Anforderungen an die Ausprägungen des Chipkartenlesers. Berücksichtigt werden kompatible Ansätze aus nationalen und internationalen Standards, Regelwerken und Richtlinien.

Abgrenzung der Technischen Richtlinie

Diese Technische Richtlinie für kontaktbehaftete und kontaktlose Chipkartenleser gilt vorrangig für Geräte zur Verwendung des Personalausweises und für weitere Kartenprojekte des Bundes, mit denen nicht-hoheitliche Anwendungen genutzt werden können. Da ein hoheitlicher Ausweisleser bei einer Personenidentifikation durch die Exekutive andere Merkmale besitzen muss, als ein Chipkartenleser für eine Authentisierung oder eine elektronische Signatur, werden diese hoheitlichen Ausweisleser in dieser Technischen Richtlinie nicht berücksichtigt.

In diesem Dokument werden für individuelle Anwendungsfälle einzelne Module basierend auf den speziellen Anforderungen des Anwendungsfalles beschrieben. Durch obligatorische und optionale Kombinationen der Module ergeben sich konkrete Ausprägungen von Chipkartenlesern, die in dieser Technischen Richtlinie spezifiziert sowie durch Prüfungsanforderungen ergänzt werden.

Die Technische Richtlinie stellt somit eine Zertifizierungsgrundlage dar.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

2 Interoperable Chipkartenleser

Diese Richtlinie definiert Kartenleser für die Verwendung mit dem elektronischen Personalausweis.

Mitunter ist es aber auch erforderlich, mit dem gleichen Chipkartenleser Chipkarten anderer Anwendungen zu unterstützen (Gesundheitskarte, Signaturkarte, Geldkarte). Daher werden im Folgenden auch Varianten von Chipkartenlesern beschrieben, die eine multifunktionale Nutzung weiterer Anwendungen erlauben.

Alle beschriebenen Chipkartenleser sind primär für den Personalausweis mit kontaktloser Kartenschnittstelle ausgelegt. Auch die kontaktbehaftete Schnittstelle wurde berücksichtigt. Nach der Einführung grundlegender Eigenschaften und Anforderungen werden in Kapitel 3 ausgesuchte Chipkartenleserklassen spezifiziert.

2.1 Terminaldefinition

Chipkartenlesegeräte können aufgrund unterschiedlicher Nutzung und unterschiedlichen Applikationen verschiedene Ausprägungen besitzen. Die Variationen beginnen bei einfachen Chipkarteninterfaces ohne Tastatur und Display bis hin zu Chipkartenlesegeräten mit eigenen Anwendungen für erweiterte sicherheitsrelevante Funktionen. Oft werden diese Chipkartenleser auch Kartenterminals genannt.

Der Übergang von einem Chipkartenleser, der im Wesentlichen für die Kommunikation zwischen Chipkarte und Host verantwortlich ist, und einem Kartenterminal mit erweiterten Funktionen ist fließend.

In dieser Richtlinie wird nicht explizit zwischen Chipkartenleser und Kartenterminal unterschieden. Es wird, unabhängig von den tatsächlichen Ausprägungen, von einem Chipkartenleser gesprochen.

2.2 Architektur

Aufgrund der Vielfalt von Chipkartenlesern und ausgehend von den eingangs verlangten interoperablen Zielen sowie als Grundlage für eine Produktqualifikation, wird eine Aufteilung der speziellen Eigenschaften eines Chipkartenlesers in einzelne Module vorgenommen. Die Ansteuerung der Chipkarte, des Lesers und auch deren funktionalen Komponenten (Tastatur, Display, usw.) erfolgt über Kommandos nach [PC/SC] und APDUs nach [ISO 7816] sowie optional anderer APIs.

Ist es bei Chipkartenlesern für den persönlichen Gebrauch noch wichtig, dass die Anwendungsprogrammierung flexibel und einfach zu entwickeln ist, so spielen bei Systemlesern andere, spezielle Anforderungen eine Rolle. Systemleser sind nicht Gegenstand dieser Version der Technischen Richtlinie.

Wenn nicht durch eine spezielle Leserausprägung ein Modul vorgeschrieben wird, können die Module **optional** verwendet werden. Wird eine Funktionalität in einem Chipkartenleser verwendet und ist diese Funktion in dieser Ausprägung des Lesers als Modul beschrieben, so muss das Modul aus Interoperabilitätsgründen umgesetzt werden. In Kapitel 3 werden speziellen Leserausprägungen dargestellt, die sich aus den Anforderungen der einzelnen Anwendungen (Use Cases) ergeben.

Allgemeine Empfehlungen werden in Kapitel 4, die Module werden im Anhang A detailliert beschrieben.

2.3 Zertifizierung

Chipkartenleser-Hersteller können beim BSI die Überprüfung der Konformität ihrer Produkte zur Technischen Richtlinie BSI TR-03119 beantragen und sich diese mit einem Zertifikat bestätigen lassen.

Voraussetzung für die Erteilung eines Zertifikats durch das BSI ist eine erfolgreich absolvierte Konformitätsprüfung gemäß den in dieser Richtlinie (Anhang B) definierten Prüfanforderungen. Konformitätsprüfungen werden dabei von unabhängigen Prüfstellen durchgeführt, die vom BSI gemäß DIN ISO/IEC 17025 aner-

kannt wurden. Die Auswahl und Beauftragung einer oder mehrerer geeigneter Prüfstellen ist Aufgabe des Antragstellers.[1]

Alle im Rahmen der Konformitätsprüfung durchgeführten Prüfungen werden von der jeweiligen Prüfstelle protokolliert und in einem abschließenden Prüfbericht zusammengefasst.

Die Zertifizierungsstelle im BSI überwacht die Konformitätsprüfung und erteilt nach erfolgreichem Abschluss auf Grundlage aller Prüfberichte das beantragte Zertifikat.

Erteilte Zertifikate werden vom BSI veröffentlicht.

Außerdem erhalten zertifizierte Chipkartenleser ein BSI-Prüfsiegel als Kennzeichen einer erfolgreichen Zertifizierung nach BSI TR-03119. Das Prüfsiegel kann nach erfolgreicher Zertifizierung gemäß den Vorgaben des BSI am Kartenleser angebracht und gemäß den Vorgaben des BSI für Werbezwecke verwendet werden.

Ist eine Zertifizierung nach BSI TR-03119 Voraussetzung für den hoheitlichen/behördlichen Einsatz eines Kartenlesers, ist dessen Kennzeichnung durch ein Prüfsiegel verpflichtend. Dies kann auch der Fall sein, wenn eine Kennzeichnung im Rahmen von Ausschreibungsverfahren o.ä. gefordert wird.

Weiterführende Informationen zum Zertifizierungsverfahren nach Technischen Richtlinien finden Sie auf den Internetseiten des BSI.

1 Eine Liste aller für die Durchführung von Konformitätsprüfungen nach Technischen Richtlinien anerkannten Prüfstellen ist auf den Internetseiten des BSI veröffentlicht.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

3 Kategorien von Chipkartenlesern

Aus Gründen der Interoperabilität und als Grundlage einer Prüfung und Bewertung haben alle Chipkartenleser die gleichen Basiseigenschaften. Je nach Anwendung sind unterschiedliche zusätzliche Funktionalitäten und auch Hardwareausprägungen bei den Chipkartenlesern erforderlich.

Im Folgenden werden drei Arten von Chipkartenlesern beschrieben.

3.1 Basis-Chipkartenleser (Cat-B)

Einfache Chipkartenleser sind oft generisch ausgeprägt, bzw. für eine bestimmte Anwendung konzipiert und unterstützen somit einige Basisfunktionen, die aber durchaus von Applikationen mit ähnlichen Anforderungen genutzt werden können.

Die Basis-Chipkartenleser (Cat-B) können im Heimbereich u.a. für folgende Dienste eingesetzt werden:

- e-Government Dienste des Personalausweises (z.B. Authentisierungsdienst, Rentenversicherung)
- Altersverifikation
- eTicketing nach VDV Kernapplikation (mit kontaktloser Karte entsprechend VDV Kernapplikation)
- Wohnsitz- und Identitätsnachweis bei Internetshopping
- Postident Ersatz

	Leserkategorie			**Modul Anhang A**	**Prüfvorschriften Anhang B**
	Cat-B	**Cat-S**	**Cat-K**		
Schnittstelle zum Host-Rechner	X	X	X	A.1	B.1
kontaktlose Schnittstelle nach ISO/IEC 14443	X	X	X	A.2	B.2
kontaktbehaftete Schnittstelle nach ISO/IEC 7816	O	O	X	A.3	B.3
PIN-Pad (sichere PIN-Eingabe) mit PACE-Unterstützung	O	X	X	A.4	B.4
Display (2x16 alphanumerische Zeichen)	O	O	X	A.5	B.5
Qualifizierte Signatur mit kontaktbehafteten Karten	O	O	X	A.6	B.6
Qualifizierte Signatur mit kontaktlosen Karten nach TR-03117 (z.B. Personalausweis)	O	O	X	A.7	B.7
Firmwareupdate	O	X	X	A.8	B.8
	X = verpflichtend; O = optional				

Tabelle 1: Übersicht Chipkartenleser-Kategorien

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

Das Lesegerät unterstützt bei diesen Anwendungen den Datenaustausch zwischen dem Trägermedium und dem jeweiligen Anwendungsserver im Internet.

3.2 Standard-Chipkartenleser (Cat-S)

Häufig findet man Chipkartenleser, die höheren qualitativen Ansprüche genügen, so konstruiert, dass sie auf dem Tisch platziert werden können und die, je nach bevorzugten Einsatzgebieten, variierende Ausprägungen (z.B. Tastatur, Display usw.) besitzen. Diese Chipkartenleser werden hier als Standard-Leser bezeichnet und besitzen mindestens ein PIN-Pad zur sicheren PIN-Eingabe.

Zusätzlich zu den Anwendungen, für die ein Cat-B-Leser geeignet ist, kann ein Standardleser (je nach Ausprägung) z.B. für folgende Anwendungen genutzt werden:

- eID-Funktion im Internet bei erhöhten Sicherheitsanforderungen
- kontaktbehaftete Anwendungen
- qualifizierte Signatur (setzt Bestätigung nach Signaturrecht voraus).

3.3 Komfort-Chipkartenleser (Cat-K)

Eine weitere Kartenleservariante ist der Komfort-Leser, welcher aufgrund der Vielfältigkeit und komfortablen Nutzungsvarianten eine Vielzahl von Anwendungen bedienen kann. Er besitzt mindestens ein PIN-Pad zur sicheren PIN-Eingabe und ein Display mit 2x16 alphanumerischen Zeichen.

Neben der kontaktlosen Schnittstelle z.B. des Personalausweises einschließlich der Signaturfunktion wird auch die kontaktbehaftete Schnittstelle klassischer Signaturkarten oder der Gesundheitskarte einschließlich der notwendigen Sicherheitsfunktionen unterstützt. Ebenso ist optional eine Unterstützung von Bankanwendungen (FinTS, Secoder) möglich.

Während die Basisleser die preisgünstige Variante darstellen, mit denen speziell für den Heimbereich dedizierte Anwendungen mit begrenztem Sicherheitslevel bedient werden können, sind Standard- und Komfortgeräte zusätzlich sicherheitstechnisch und funktionell für Anwendungen mit erweiterten Sicherheitsfunktionen ausgelegt.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

4 Allgemeine Empfehlungen

Dieses Kapitel enthält allgemeine Empfehlungen für die Eigenschaften eines Kartenlesers. Die Empfehlungen sind nicht verpflichtend und nicht Bestandteil der Konformitätsprüfung. Der Prüfungsumfang für die einzelnen Module wird in Anhang B festgelegt.

4.1 Nutzungsprozesse und Use Cases

Die Spezifikation der Geräte muss alle Use Cases im Lebenszyklus des Chipkartenlesers in Betracht ziehen. Dabei sind die folgenden Besonderheiten zu beachten:

1. Die Installation des Geräts wird normalerweise durch den Anwender durchgeführt.
2. Wenn der Leser ein Firmwareupdate unterstützt und im Laufe der Zeit ein Firmwareupdate notwendig sein sollte, muss das Update vom Endanwender in einem einfachen Verfahren in den Leser eingebracht werden können.
3. Im Laufe der Zeit werden je nach Dienst, der genutzt werden soll, anwendungsspezifische Softwarpakete installiert. Dies gilt für den Fall des erstmaligen Nutzens als auch für Updates.
4. Grundsätzlich soll eine beliebige Zahl von Diensten unterschiedlicher Anbieter gleichzeitig nutzbar sein.
5. Sobald ein Dienst nicht mehr benötigt wird, soll die dienstespezifische Software deinstalliert werden.

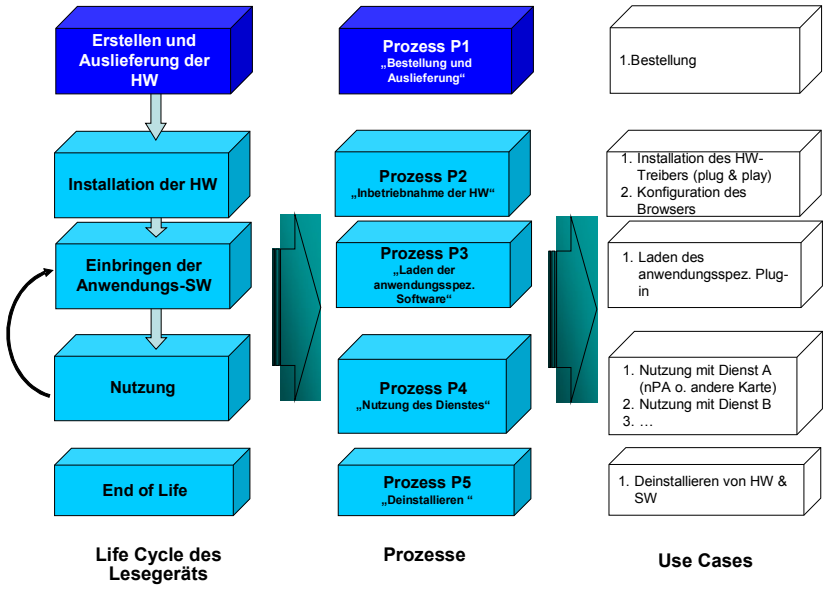

Abbildung 1: Life Cycle der generischen Lesegeräte

Abbildung 1 zeigt den Lebenszyklus eines generischen Chipkartenlesers und die zugeordneten Betriebsprozesse und Use Cases. Die Use Cases müssen bei der Spezifizierung der Hard- und Software des Lesegerätes abgedeckt werden.

4.2 Grundlagenanforderungen und Annahmen

Grundsätzlich sind die gesetzlichen und weiteren regulatorischen Anforderungen einzuhalten, wie z.B. EMV-Grenzwerte, CE-Kennzeichnung oder Entsorgungsverpflichtungen gemäß der EU-Vorgaben.

Bei der konkreten Ausgestaltung eines Kartenlesegerätes auf Basis dieser Richtlinie sollten verschiedene Anforderungen und Überlegungen berücksichtigt werden:

- **Optimierung des Verhältnisses von Kosten und Nutzen**: Je nach Verwendungszweck sind unterschiedliche Ausstattungsmerkmale notwendig, so müssen, z.B. Kosten und Nutzen eines PIN-Pads oder einer Anzeige anwendungsbezogen gegeneinander abgewägt werden.
- **Anwenderfreundlichkeit**: Das Lesegerät muss auch durch Laien problemlos am PC zu installieren sein. Dies betrifft insbesondere die Basis-Chipkartenleser.
- **Fehlertoleranz**: Bei Ausfall von Hardwarekomponenten, die von der Logik des Kartenlesers diagnostizierbar sind, sollte der Chipkartenleser nicht in einen undefinierten Zustand schalten, sondern mit Abbruch und/oder Fehlermeldungen reagieren.
- **Support**: Für den Fall von technischen Problemen muss dem Anwender eine einfache Möglichkeit zur Prüfung seines Chipkartenlesers mit nPA und – bei weiterführendem Support-Bedarf - ein technischer Kundenservice zur Verfügung stehen.
- **Betriebssysteme**: Um den Anwender nicht unnötig einzuschränken, sollen möglichst viele Betriebssysteme unterstützt werden, d.h. es müssen entsprechende Treiber einschließlich der notwendigen Updates zur Verfügung stehen.
- **Sicherheit eines PIN-Pads**: Sofern der Leser ein eigenes PIN-Pad besitzt, so muss dieses sicher gestaltet werden. Dies bedeutet z.B., dass die eingegebene PIN weder zum Host-Rechner übertragen werden darf noch ungeschützt zur Karte (insbesondere bei Verwendung einer kontaktlosen Schnittstelle) übertragen wird.
- **Sicherheit eines Anzeigemoduls**: Eine integrierte Anzeige – sofern vorhanden – soll genutzt werden, um den Anwender mit sicheren Informationen zu versorgen. Bei Nutzung der eID-Funktion des Personalausweises umfasst dies z.B. die Berechtigungen und den Namen des Dienstanbieters.
- **Kryptographische Verfahren**: Sofern im Kartenleser kryptographische Verfahren implementiert werden (z.B. PACE), so müssen diese Verfahren sicher implementiert werden. Dies betrifft sowohl die korrekte und sichere Implementierung der Kryptographie selbst als auch z.B. die sichere Erzeugung von Schlüsselmaterial (Zufallszahlen).
- **Manipulationsschutz**: Der Endbenutzer sollte erkennen können, dass das Gerät nicht manipuliert wurde. Dies betrifft insbesondere Kartenleser mit eingebauten Sicherheitsfunktionen wie z.B. PIN-Pad oder Tastatur.
- **Prüfungen**: Werden weitere Anwendungen unterstützt, z.B. gematik-Anwendungen, VDV-Kernapplikation oder Bankanwendungen, so empfiehlt sich die Prüfung der Interoperabilität entsprechend der zugehörigen Prüfstandards. Diese Prüfungen sind nicht Bestandteil dieser Richtlinie.

Diese Anforderungen sollten bei der Auswahl der Funktionsmodule und deren Implementierung berücksichtigt werden.

4.3 Schnittstellen

Ein Chipkartenleser bildet das Bindeglied zwischen Chipkarte, Host-Rechner und Benutzer und bietet dementsprechend Schnittstellen mindestens zu diesen an. Sofern Schnittstellen implementiert werden, die über die in Anhang A definierten Module hinausgehen, empfiehlt das BSI die Prüfung dieser Schnittstellen auf Basis der entsprechenden Prüfvorschriften.

4.3.1 Schnittstelle zur Chipkarte

In Anhang A werden Module für die kontaktlose Schnittstelle nach [ISO 14443] und für die kontakbehaftete Schnittstelle nach [ISO 7816] als Basisschnittstellen für Kartenleser gemäß dieser Richtlinie definiert.

4.3.1.1 EMV-Unterstützung

Optional können Applikationen des Kreditwesens unterstützt werden. Maßgeblich sind hierzu die Anforderungen des [EMV] Standards. Da dieser Standard nicht kompatibel zu [ISO 7816] ist, ist eine Umschaltmöglichkeit im Chipkartenleser durch die Anwendung auf dem Host-Rechner vorzusehen, falls beide Standards unterstützt werden. In diesem Fall ist die Umschaltung zwischen EMV-Modus und ISO-Modus durch den Hersteller im Betriebshandbuch oder dem Programmierhandbuch zu beschreiben.

4.3.1.2 Synchrone Chipkarten

Neben asynchronen Chipkarten können für die kontaktbehaftete Schnittstelle auch synchrone Chipkarten unterstützt werden.

Erhält der Chipkartenleser nach Stecken einer kontaktbehafteten Chipkarte keinen ATR entsprechend [ISO 7816], part 3, wird eine synchrone Chipkarte in der Kontaktiereinheit angenommen. Der Chipkartenleser initiiert daraufhin eine Aktivierung der Chipkarte nach den Konventionen für synchrone Chipkarten. Die ersten 32 Taktzyklen interpretiert der Chipkartenleser als den vier Byte langen ATR einer synchronen Chipkarte nach [ISO 7816], part 10, und stellt im Erfolgsfall das Protokoll zur Datenkommunikation entsprechend ein. Bei Misserfolg versucht der Chipkartenleser die Kommunikation mit der Chipkarte ohne Resetfunktion nach dem I²C-Bus-Protokoll aufzubauen. Ist auch das nicht erfolgreich, werden die Kontakte gemäß den Anforderungen der [ISO 7816], part 3, deaktiviert.

4.3.2 Schnittstelle zum Host-Rechner

Die grundlegende Schnittstelle zwischen Kartenleser und Host-Rechner ist PC/SC (siehe Modul A.1). Darüber hinaus können weitere Schnittstellen unterstützt werden, z.B [MKT] für synchrone Karten im Bereich des Gesundheitswesens.

4.3.3 Schnittstelle zum Nutzer

Chipkartenleser können über verschiedene Schnittstellen zum Bediener verfügen. PIN-Pad und Display werden in den Modulen A.4 bzw. A.5 spezifiziert.

Falls eine Eingabetastatur vorhanden ist, sollten folgende Regelungen beachtet werden:

- Bei einer 12er-Tastatur sollten die 11. und 12. Taste als Abbruchtaste und Bestätigungstaste belegt werden;

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

- wird eine 16er-Tastatur verwendet sollte zusätzlich eine Korrekturtaste vorgesehen werden.

Auf eine ergonomisch günstige Ausprägung der Tastatur und eine barrierefreie Ausführung, z. B. durch ein fühlbares Tastenfeld oder durch Brailleschrift, sollte geachtet werden. Die Anordnung der Tasten kann in Anlehnung an [CEN 1332], Teil 5, erfolgen.

Darüber hinaus kann der Kartenleser weitere Bedienerschnittstellen aufweisen, einige werden im folgenden beispielhaft aufgezählt.

4.3.3.1 Leuchtdioden

Der Chipkartenleser ist nach Anlegen der Versorgungsspannung betriebsbereit. Eine Leuchtdiode in einer ersten Farbe (vorzugsweise grün) signalisiert den Zustand nach einer korrekten Initialisierung des Chipkartenlesers. Der Betriebszustand nach Aktivierung (kontaktbehaftet) oder Selektierung (kontaktlos) der Chipkarte wird durch eine Leuchtdiode (nach Möglichkeit) in einer zweiten Farbe (vorzugsweise gelb) angezeigt. Sofern zwischen den Schnittstellen unterschieden werden soll, so sollte gelb für die kontaktbehaftete und blau für die kontaktlose Schnittstelle vorgesehen werden. Eine blinkende Leuchtdiode in der zweiten Farbe oder einer dritten Farbe signalisiert den Fehlerfall.

Mindestens eine Leuchtdioden-Anzeige sollte vorhanden sein. Diese zeigt mindestens an, wenn eine Chipkarte aktiviert oder selektiert ist. Die Bereitschaft des Lesers sollte ebenfalls dem Bediener angezeigt werden. Ausnahmen können gemacht werden, wenn die Bauform (z. B. integrierter Chipkartenleser) keine Möglichkeiten für eine Leuchtdiodenanzeige bieten.

4.3.3.2 Anzeige des Sicherheitsmodus

Sicherheitstechnische Applikationen erfordern authentische Ein- und Ausgaben.

So wird beispielsweise dem Benutzer signalisiert, dass die über die Tastatur des Chipkartenlesers eingegebene Geheimzahl nicht in die unsichere Umgebung des Personalcomputers oder über offene Übertragungswege an den Host-Rechner gelangt. Auch Ausgaben, die zum Beispiel bei einer digitalen Signatur oder einem Bezahlvorgang auftreten, können eine authentische Anzeige voraussetzen.

Um zu informieren, dass der Chipkartenleser sich im gesicherten Modus befindet, ist dieses dem Anwender eindeutig zu signalisieren. Dazu sind akustische, optische oder andere deutlich wahrnehmbare Signale zur Verfügung zu stellen. Zusatzleuchten und Symbole in Displays sind derzeit gängige Anzeigen. Es sollte beachtet werden, dass eine barrierefreie Unterstützung der Funktion, z. B. durch vergrößerte Symbole oder eine Kombination von optischen und akustischen Anzeigen, gewährleistet ist.

Dabei ist sicherzustellen, dass das Signal nicht unbefugt ansteuerbar ist und nur von der Firmware des Chipkartenlesers bedient wird.

Die Nutzung der Signalisierung ist dem Benutzer in der Dokumentation eindeutig darzustellen.

4.3.3.3 Biometrischer Sensor

Der Chipkartenleser kann zusätzlich einen oder auch mehrere biometrische Sensoren besitzen. Möglichkeiten sind beispielsweise Fingerabdruck, Spracherkennung oder Irisabtastung zur Identifikation biometrischer Merkmale.

Die biometrischen Daten dürfen nicht in die Umgebung des Hosts-Rechners gelangen.

Es werden in dieser Richtlinie keine weiteren Kriterien für die Funktion und Sicherheit der biometrischen Systeme angeführt.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

A Module

Die nachfolgenden Module dienen zur interoperablen und kompatiblen Nutzung verschiedener Chipkartenleser. Durch obligatorische und optionale Kombinationen der Module ergeben sich konkrete Leserausprägungen, daher müssen nicht in jedem Chipkartenleser alle Module berücksichtigt werden.

Ebenso kann der Leser Eigenschaften/Funktionen unterstützen, die nicht in einem der Module definiert wird. Falls jedoch die Ausprägung oder die Funktionseinheit vorhanden ist, so sind ausschließlich die anschließend definierten Modulbeschreibungen zu berücksichtigen.

Werden Kommandos zur Steuerung des Chipkartenlesers benötigt (z.B. PIN-Eingabe) so dürfen keine proprietären Kommandos, sondern es müssen die hier aufgeführten Terminalkommandos verwendet werden.

A.1 Schnittstelle zum Host-Rechner

A.1.1 PC/SC

Der Kartenleser wird über [PC/SC] angesprochen. PC/SC ist ein von der PC/SC-Workgroup entwickelter Standard für den Zugriff auf ein Kartenlesegerät. Fehlen spezielle Ansteuerungsmöglichkeiten, so bietet PC/SC einen transparenten Kanal für proprietäre Kommandos.

Bei PC/SC für Windows Umgebungen sind WHQL Zertifikate von Microsoft erforderlich.

A.1.2 Leserinformationen

Die PC/SC Treiber des Chipkartenlesers müssen Kommandos zum Auslesen von

- Herstellername
- Produktname
- Firmwareversion
- Treiberversion

unterstützen. Die Kommandos sind in Tabelle 2 aufgeführt.

Kommando	Beschreibung
0xFF-0x9A-0x01-0x01-0x00	Herstellername
0xFF-0x9A-0x01-0x03-0x00	Produktname
0xFF-0x9A-0x01-0x06-0x00	Firmwareversion
0xFF-0x9A-0x01-0x07-0x00	Treiberversion[2]

Tabelle 2: Kommandoübersicht GetReaderInfo

Beispiel:

Kommando: 0xFF-0x9A-0x01-0x01-0x07-0x00

2 Sofern der Kartenleser von den Betriebssystemen nach A.1.3 ohne Treiber unterstützt wird und mit dem Kartenleser keine Treiber ausgeliefert werden, so wird als Version für den Treiber der String „CCID“ zurückgegeben.

Antwort: 0x31-0x2e-0x30-0x31-0x90-0x00 („1.01“)

Diese Kommandos sind für alle Schnittstellen zu implementieren.Sie müssen jedoch nur unterstützt werden, wenn eine Chipkarte an der entsprechenden Schnittstelle verfügbar ist. Die Implementierung der Funktionalität ohne vorhandene Karte ist optional.

A.1.3 Betriebssysteme

Der Kartenleser muss die folgenden Betriebssysteme unterstützen:

- Windows
- MacOS X
- Linux (z.B. Debian, Ubuntu, OpenSuse)

Es ist jeweils mindestens eine der zum Zeitpunkt der Antragstellung vom Betriebssystemhersteller unterstützten Betriebssystemversionen zu unterstützen. Stehen Versionen für 32 Bit und 64 Bit zur Verfügung, so sind beide zu unterstützen. Die unterstützten Betriebssysteme sind durch den Kartenleserhersteller klar zu kennzeichnen.

Ein Update der Schnittstellentreiber auf zukünftige und weitere Versionen der Betriebssysteme muss möglich sein und vom Lieferanten auf Anforderung bereitgestellt werden.

Ausgenommen von dieser Anforderung sind untrennbar mit dem Host-Rechner verbundene Kartenleser (integriertes System), sofern die Unterstützung eines oder mehrerer der oben genannten Betriebssysteme technisch nicht möglich oder aus rechtlichen Gründen nicht zulässig ist.

Beispiele für integrierte Systeme sind Notebooks, Netbooks, SmartPads, Mobiltelefone, POS-Zahlungterminals sowie Verkaufsautomaten. Die technische Unmöglichkeit bzw. die rechtliche Nichtzulässigkeit der Unterstützung ist für jedes Betriebssystem aus der oben genannten Liste, das nicht unterstützt wird, gesondert zu belegen.

A.2 Kontaktlose Schnittstelle

Kontaktlose Chipkartenleser erfüllen die Anforderungen gemäß [ISO 14443], parts 2, 3 und 4[3].

Der Chipkartenleser unterstützt die Protokolltypen Typ A und Typ B nach [ISO 14443], part 2.

Als Transportprotokoll wird unterstützt:

- T=CL, Block orientiertes Halbduplex-Protokoll nach [ISO 14443], part 4, einschließlich „Protocol and parameter selection“ (PPS).

Es müssen mindestens die Übertragungsgeschwindigkeiten 106, 212 und 424 kbit/s nach [ISO 14443], part 2, unterstützt werden.

Der Kartenleser muss für die kontaktlose Schnittstelle Karten im Format td-1 (85,6 mm x 54,0 mm x 1,25mm) nach [ICAO 9303], part 3, volume 1, unterstützen. Dabei ist für die Dicke eine Unterstützung des Bereichs 800µm bis 1100µm (Kartendicke 800µm bis maximal 900µm; Adressaufkleber mit Schutzfolie maximal 200µm) ausreichend.

Sofern eine kontaktbehaftete Schnittstelle unterstützt wird (Modul A.3), so ist es bei der Umstellung von kontaktbehafteten Karten auf kontaktlose Karten erforderlich, bei einem Reset einen [ISO 7816], part 3, konformen ATR an die Applikation zu melden.[4] Dies ist spezifiziert in [PC/SC], part 3.

3 Hinweis: Gemäß der aktuellen Version der [ISO 14443], part 3, bedeutet dies insbesondere eine Mindestfeldstärke von 2A/m für das vom Leser erzeugte Feld.

A.3 Kontaktbehaftete Schnittstelle

Multifunktionale Lesertypen können zusätzlich auch kontaktbehaftete Chipkarten unterstützen.Solche Leser besitzen mindestens eine Kontaktiereinheit zur Aufnahme von Chipkarten der Größe ID-1 (85,6 mm x 54,0 mm x 0,80 mm) entsprechend [ISO 7810]. Sofern für die kontaktlose Schnittstelle nach Modul A.2 und die kontaktbehaftete Schnittstelle der gleiche Kartenschacht genutzt wird, so muss insbesondere darauf geachtet werden, dass die Kontaktiereinheit Karten im Format td-1 (siehe auch Modul A.2) nicht beschädigt. Werden verschiedene Kartenschächte genutzt und ist der kontaktbehaftete Schacht für Karten im Format td-1 nicht geeignet, so muss darauf in der Dokumentation zum Leser explizit hingewiesen werden.

Die Lage und die Zuordnung der Kontakte ergibt sich aus [ISO 7816], part 2.

Darüber hinaus kann der Chipkartenleser optional weitere Kontaktiereinheiten besitzen. Diese können auch für das Format ID-000 (Plug-in-Karte) nach [ISO 7810] ausgelegt sein.

Die Kontakte des Chipkartenlesers müssen gegen Kurzschlüsse einzelner oder aller Kontakte gegeneinander resistent sein. Nach Kurzschlüssen an den Kontakten muss die Funktion des Chipkartenlesers in vollem Umfang wiederherstellbar sein. Es dürfen keine irreversiblen Schäden auftreten.

Der Chipkartenleser beliefert die Chipkarte standardmäßig mit einer Versorgungsspannung von 5 V, der Class A nach [ISO 7816], part 3. Optional ist die Unterstützung einer zusätzlich niedrigeren Versorgungsspannung zum Stromsparen. Diese Ausprägung entspricht der Class B und Class C für 3 V und 1,8 V Chipkarten gemäß [ISO 7816], part 3.

Der Betrieb von asynchronen, kontaktbehafteten Chipkarten durch den Chipkartenleser erfolgt konform zu [ISO 7816], part 3. Dazu gehören:

- Aktivierung der Chipkarte
- Verhalten und Konfiguration während ATR („answer to reset“)
- Protokoll-Parameter-Auswahl PPS („protocol and parameter selection“)
- Informationsaustausch mit der Chipkarte
- Deaktivierung der Chipkarte

Die Unterstützung von PPS und die damit verbundene Protokoll- und Parameter-Auswahl ist in Übereinstimmung mit der [ISO 7816], part 3, zur Erzielung höherer Datenübertragungsraten erforderlich.

Nach Einführung einer Chipkarte in den Chipkartenleser geht diese zunächst von einer asynchronen Chipkarte aus. Ein Reset-Kommando an den Chipkartenleser führt eine Aktivierungssequenz und eine Auswertung des ATR („Answer to reset“) nach [ISO 7816], part 3, aus. Bei fehlendem oder inkorrekt empfangenem ATR einer asynchronen Chipkarte kann die Aktivierung vom Chipkartenleser noch maximal zweimal wiederholt werden.

Unterstützt werden die folgenden Transportprotokolle:

- T=1, Block orientiertes Halbduplex-Protokoll nach [ISO 7816], part 3
- T=0, Zeichen orientiertes Halbduplex-Protokoll nach [ISO 7816], part 3

4 Hinweis: Gemäß [TR-03110] kann der Sicherheitszustand eines Personalausweises durch ein SELECT MF ohne Secure Messaging zurückgesetzt werden. Dies wird von den derzeit produzierten Ausweisen noch nicht unterstützt. Ein Zurücksetzen des Sicherheitszustandes nach einer durchgeführten Authentisierung ist bei diesen Karten nur durch Ab-/Anschalten des Lesefeldes möglich. Dies kann durch den Kartenleser über das PC/SC-Kommando SCardReconnect mit SCARD_RESET_CARD unterstützt werden. Dabei sollte dem Host-Rechner keine neue Karte signalisiert werden.

A.4 PIN-Pad mit PACE-Unterstützung

Der Chipkartenleser kann eine Tastatur besitzen. In diesem Modul werden die Anforderungen an ein PIN-Pad (einschließlich der Anforderungen, die sich aus der PACE-Unterstützung ergeben) formuliert.

A.4.1 Sichere PIN-Eingabe

Die PIN wird direkt über die Tastatur des Kartenlesers an die Chipkarte übertragen, die Daten verlassen nicht das Terminal. Die Verifikation der PIN findet auf der Karte statt. Damit wird ein höheres Sicherheitsniveau für die PIN im Vergleich zu Kartenlesern ohne PIN-Pad erreicht. Bei Letzteren besteht grundsätzlich die Möglichkeit, dass z.B. ein Keylogger auf dem Host-Rechner die PIN mitliest.

Bei einem kontaktlosen Chipkartenleser wird zur Absicherung der Datenkommunikation über die Luftschnittstelle das PACE-Protokoll benutzt.

Unterstützt der Leser neben der sicheren PIN-Eingabe auch eine nicht-sichere PIN-Eingabe (z.B. eine PIN-Eingabe am Host-Rechner für bestimmte Anwendungen), so muss dies dem Nutzer eindeutig angezeigt werden (vgl. auch 4.3.3.2). Eine nicht-sichere PIN-Eingabe darf nur für Anwendungen vorgesehen werden, wo dies in den entsprechenden Spezifikationen vorgegeben ist. Die Signalisierung darf nicht vom Host-Rechner ansteuerbar sein.

Eine eingegebene PIN ist nach Verwendung unmittelbar zu löschen bzw. zu überschreiben.

A.4.2 PACE

Das PACE-Verfahren dient dem Aufbau eines sicheren Kanals zwischen Lesegerät und Chipkarte. Bei Verwendung eines Lesers mit PIN-Pad wird PACE direkt im Kartenterminal ausgeführt.

Für dieses Modul werden die folgenden in Anhang D definierten Kommandos genutzt:

- GetReaderPACECapabilities
- EstablishPACEChannel

Der Leser muss die Capabilities PACE und eID unterstützen.

Der Kartenleser muss dabei die kryptographischen Verfahren und Schlüssellängen nach [TR-03116], Teil 2, beherrschen. Aus Gründen der Zukunftssicherheit kann es sinnvoll sein, auch weitere Schlüssellängen zu unterstützen.

A.4.3 PACE Schlüsselerzeugung

Für den Einsatz von PACE als Sicherungsverfahren muss durch einen geeigneten Zufallszahlengenerator eine Zufallszahl erzeugt werden.

Es muss ein Pseudozufallszahlengenerator verwendet werden, der mindestens der Klasse K3 im Sinne der [AIS 20] angehört und bei dem die Entropie des Seeds mindestens 100 Bit beträgt.

A.4.4 PIN-Management

Das Ändern der eID-PIN erfolgt durch die Verifikation der bestehenden eID-PIN mittels EstablishPACEChannel(Passwort=eID-PIN, Rolle=unauthenticated) und anschließendem Setzen einer neuen eID-PIN mittels FEATURE_MODIFY_PIN_DIRECT gemäß [PC/SC], part 10.

Zur Abfrage des Fehlbedienungszählers der eID-PIN wird das Kommando MSE:SetAT in der Kodierung für den Start des PACE-Protokolls in der Rolle eines „unauthenticated Terminal“ genutzt. Das Lesegerät muss sicherstellen, dass die Abfrage des Fehlbedienungszählers durch den Host-Rechner mit Hilfe dieses Kommandos möglich ist, aber kein vollständiges PACE-Protokoll durch den Host-Rechner durchgeführt werden kann.

Zum Zurücksetzen des Fehlbedienungszählers ist EstablishPACEChannel(Passwort=PUK, Rolle=unauthenticated) mit anschließendem RESET RETRY COUNTER zu unterstützen.

A.4.5 Filterregeln

Um zu verhindern, dass die PIN-Eingabe am PIN-Pad umgangen wird, muss der Kartenleser bestimmte Kommandos filtern, d.h. darf die Ausführung nicht zulassen bzw. darf die Kommandos nicht zur Karte weiterschicken. Dies bedeutet:

- Es muss verhindert werden, dass PACE durch den Host-Rechner durchgeführt wird.
- EstablishPACEChannel darf nicht mit vom Host-Rechner vorgegebener eID-PIN oder PUK durchgeführt werden, die Eingabe dieser Geheimnisse ausschließlich am PIN-Pad muss erzwungen werden.
- Es müssen die folgenden Kombinationen von Rolle und Passwort unterstützt werden:
  - „unauthenticated Terminal“ mit CAN, PUK und eID-PIN
  - Authentisierungsterminal mit CAN und eID-PIN
  - falls Modul A.7 (QES mit kontaktlosen Karten) implementiert wird: Signaturterminal mit CAN, eID-PIN und PUK.

  Alle anderen Kombinationen müssen gefiltert werden.
- Es muss verhindert werden, dass die eID-PIN durch den Host-Rechner geändert wird (RESET RETRY COUNTER).

Weitere Filterungen sind zulässig, solange die Funktionsfähigkeit des Lesegerätes nicht beeinträchtigt wird.

A.4.6 Manipulationsschutz

Das PIN-Pad muss so gestaltet werden, dass eine Manipulation des PIN-Pads wirksam verhindert wird oder eine Manipulation durch den Inhaber erkannt werden kann. Das erforderliche Schutzniveau orientiert sich hierbei an den Vorgaben des Signaturrechts.

A.5 Display

Ein Display muss mindestens 2 Zeilen mit je mindestens 16 Zeichen zur Darstellung umfassen.

Als Zeichenvorrat sind Groß- und Kleinbuchstaben inklusive Umlaute sowie die Sonderzeichen entsprechend DIN 66003 zu unterstützen. Außer der deutschen Sprachanzeige können weitere Sprachen zur Anzeige von Meldetexten implementiert werden. Weitere Symbole und Zeichen zur Benutzerführung (z. B. Sicherheitsmodus) sind erlaubt.

Bei Anzeigetexten mit nachfolgender Tastatur-Eingabe soll ein blinkendes Cursor-Zeichen die Position des Cursors anzeigen.

Die folgenden Standardtexte müssen im Kartenleser vorgehalten werden. Dabei sind die Texte sinngemäß zu verstehen, die konkrete Formulierung kann abweichen.

Nr.	*Text*
1	Bitte Karte bereitstellen
2	Bitte Karte entfernen
3	Karte unlesbar. Falsche Lage?
4	Bitte Geheimzahl eingeben
5	Aktion erfolgreich
6	Geheimzahl falsch/gesperrt
7	Neue Geheimzahl eingeben
8	Eingabe wiederholen
9	Geheimzahl nicht gleich. Abbruch
10	Bitte Eingabe bestätigen
11	Bitte Dateneingabe
12	Abbruch

Tabelle 3: Standard-Anzeigetexte

Der Kartenleser muss eindeutig signalisieren, ob die angezeigten Informationen authentisch vom Lesegerät selbst erzeugt wurden oder vom Host-Rechner angesteuert werden (vgl. auch 4.3.3.2).

A.5.1 eID-Nutzung

Der Kartenleser muss die authentische Anzeige von Berechtigtem und Berechtigungen gewährleisten. Das heißt insbesondere, dass diese Angaben dem Berechtigungszertifikat entnommen werden müssen, das anschließend zur Verifikation im Rahmen der Terminalauthentisierung an den Personalausweis weitergereicht werden.

Für dieses Modul werden die folgenden in Anhang D definierten Kommandos genutzt:

- GetReaderPACECapabilities
- EstablishPACEChannel.

Der Leser muss die Capabilities PACE und eID unterstützen.

A.5.2 Manipulationsschutz

Das Display muss so gestaltet werden, dass eine Manipulation des Displays wirksam verhindert wird oder eine Manipulation durch den Inhaber erkannt werden kann. Das erforderliche Schutzniveau orientiert sich hierbei an den Vorgaben des Signaturrechts.

A.6 QES mit kontaktbehafteten Karten

Das Lesegerät muss die Vorgaben des Signaturgesetzes und der Signaturverordnung einhalten.

A.7 QES mit kontaktlosen Karten gemäß TR-03117

Dieses Modul stellt die notwendigen Protokolle und Lesereigenschaften für die Erzeugung qualifizierter Signaturen mit kontaktlosen Karten gemäß [TR-03117] (z.B. Personalausweis) zur Verfügung. Das Erzeugen eines qualifizierten Schlüsselpaares bzw. Nachladen eines qualifizierten Zertifikates erfolgt in der Rolle eines Authentisierungsterminals und ist somit nicht Gegenstand dieses Moduls.

Der Kartenleser muss die leserseitigen Teile der folgenden Protokolle umsetzen. Der genaue Ablauf wird in [TR-03110] und [TR-03117] beschrieben.

Für dieses Modul werden die folgenden in Anhang D definierten Kommandos genutzt:

- GetReaderPACECapabilities
- EstablishPACEChannel.

Der Leser muss die Capabilities PACE und eSign unterstützen.

Der Kartenleser muss dabei die kryptographischen Verfahren und Schlüssellängen nach [TR-03116], Teil 2, beherrschen. Aus Gründen der Zukunftssicherheit kann es sinnvoll sein, auch weitere Schlüssellängen zu unterstützen.

A.7.1 PACE

Durchführung von PACE mit der Kartenzugangsnummer (CAN) als Passwort. Die CAN kann entweder über das PIN-Pad des Lesers eingegeben werden oder bereits vorher dem Leser bekannt sein (d.h. im Leser oder der Signatursoftware gespeichert).

A.7.2 Terminalauthentisierung

Für den Zugriff auf die Signaturfunktion weist sich der Kartenleser über die Terminalauthentisierung der Karte gegenüber als bestätigtes Signaturterminal aus. Zur Durchführung der Terminalauthentisierung muss der Leser einen privaten Schlüssel besitzen und mit diesem eine Signatur erzeugen können. Der zugehörige öffentliche Schlüssel muss vom DV-eSign der EAC-PKI signiert sein.

Die Zertifizierung der Leser durch den DV-eSign erfolgt im Rahmen der Bestätigung durch eine Bauartzertifizierung, d.h. alle Leser der gleichen (bestätigten) Bauart erhalten das gleiche Zertifikat und den gleichen privaten Schlüssel. Dieser Schlüssel wird vom Hersteller erzeugt und sicher gespeichert. Die sichere Speicherung sowie das sichere Einbringen des Schlüssels in die Leser ist Bestandteil der Evaluierung im Rahmen der Bestätigung. Nach erfolgter Bestätigung des Lesertyps wird der öffentliche Schlüssel durch das BSI zertifiziert.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

Zur Rezertifizierung stellt der Hersteller einen neuen Zertifikatsrequest für den bereits vorhandenen privaten Schlüssel an das BSI. Voraussetzung einer erneuten Zertifizierung ist die weiterhin bestehende Bestätigung des Lesers und die weiterhin ausreichende Schlüssellänge des privaten Schlüssels nach [TR-03116], Teil 2.

Ist die Schlüssellänge nicht mehr ausreichend, bestehen zwei Möglichkeiten:

1. Bereits im Herstellungsprozess werden mehrere private Schlüssel verschiedener Längen eingebracht, von denen einer geeignet zur Zertifizierung ist
2. Der Leser ist in der Lage, einen neuen Schlüssel auf sicherem Wege zu importieren.

Nähere Informationen zur Zertifizierung durch den DV-eSign siehe [CP-eSign].

A.7.3 Passive Authentisierung

Der Leser liest die Datei EF.CardSecurity und prüft die darin enthaltene Signatur. Zur Überprüfung der Signatur muss eine Zertifikatskette überprüft werden, deren Wurzel das CSCA-Zertifikat des BSI ist. Der Kartenleser muss das CSCA-Zertifikate manipulationssicher speichern. Alle weiteren notwendigen Daten und Zertifikate sind auf dem Ausweis selbst gespeichert.

Bei Wechsel des CSCA-Zertifikates durch das BSI (etwa alle 2-3 Jahre) muss das neue Zertifikat (zusätzlich) dem Leser bekannt gemacht werden und dort für Signaturprüfungen vorgehalten werden. Ein sicherer Import des Zertifikates ist nicht notwendig, da das neue Zertifikat mittels des alten Wurzelzertifikates überprüft werden kann. Die Festlegungen zu den Schlüssellängen nach [TR-03116], Teil 2, sind zu beachten.

A.7.4 Chipauthentisierung

Mittels des aus der Datei EF.CardSecurity ausgelesenen und mit der Passiven Authentisierung verifizierten öffentlichen Schlüssel des Chips wird ein neuer sicherer Kanal (Secure Messaging) zwischen Leser und Ausweis aufgebaut, der den PACE-Kanal ablöst.

A.7.5 Signatur-PIN

Für den Umgang mit der Signatur-PIN muss der Kartenleser die folgenden PC/SC-Kommandos nach [PC/SC], part 10, implementieren und in entsprechende Kommandos/Kommandofolgen nach [TR-03117] umsetzen.

- Die Verifikation der Signatur-PIN wird vom Host-Rechner mit FEATURE_VERIFY_PIN_DIRECT ausgelöst. Dieses Kommando darf für die kontaktlose Schnittstelle nur nach erfolgreicher Durchführung von EstablishPACEChannel(Passwort=CAN, Rolle=Signaturterminal) unterstützt werden.
- Ein Ändern der Signatur-PIN wird über FEATURE_MODIFY_PIN_DIRECT ausgelöst. Dieses Kommando darf für die kontaktlose Schnittstelle nur nach erfolgreicher Durchführung von EstablishPACEChannel(Passwort=CAN, Rolle=Signaturterminal) unterstützt werden.
- Ein Neusetzen der Signatur-PIN wird über FEATURE_MODIFY_PIN_DIRECT ausgelöst. Dieses Kommando darf für die kontaktlose Schnittstelle nur nach erfolgreicher Durchführung von EstablishPACEChannel(Passwort=eID-PIN, Rolle=Signaturterminal) unterstützt werden.
- Ein Zurücksetzen des Fehlbedienungszählers erfolgt über das Kommando CHANGE REFERENCE DATA gemäß [TR-03117] nach Durchführung von EstablishPACEChannel(Passwort=PUK, Rolle=Signaturterminal).

A.7.6 Filterregeln

Ein Neusetzen/Ändern/Nutzen der Signatur-PIN darf ausschließlich über die beschriebenen Kommandos erfolgen, d.h. insbesondere, dass der Kartenleser Kommandos des Host-Rechners, die auf die Signatur-PIN zugreifen (insbesondere VERIFY und CHANGE REFERENCE DATA), filtern muss.

A.7.7 Signaturerzeugung

Die Erzeugung der Signatur erfolgen mit Standard-Kommandos nach ISO 7816, wie in [TR-03117] beschrieben.

A.8 Firmware-Update

Werden Chipkartenleser gefordert, bei denen Leistungsanpassungen auf Grund veränderter Umgebungsbedingungen notwendig werden können, müssen die Chipkartenleser mit einer Secure-Download-Funktion ausgestattet sein. Die Firmware des Chipkartenlesers ist elementare Grundlage für die Sicherstellung der geprüften Leistungsmerkmale.

Die Download-Funktion kann mit einem separaten Ladeprogramm durchgeführt werden, das für die verschiedenen Systemumgebungen bereitgestellt wird.

Sofern die Firmware Sicherheitsleistungen erbringt (d.h. sofern der Leser eines der Module A.4 – A.7 implementiert), ist der Download-Vorgang so abzusichern, dass die Chipkarten-Firmware nicht unbefugt verändert werden kann. Mit einem kryptographischen Sicherungssystem muss sichergestellt werden, dass nur autorisierte Personen oder Systeme an den Leistungsmerkmalen des Chipkartenlesers Veränderungen vornehmen können. Die Integrität und Vollständigkeit der neuen Daten muss durch die Firmware des Lesers selbst überprüft werden. Es muss eine Absicherung über eine digitale Signatur der Daten erfolgen. Die spätere Anwendung bestimmt die Höhe des Sicherheitslevels an dieser Stelle.

B Prüfanforderungen

In diesem Anhang werden die Prüfanforderungen zu den jeweiligen Modulen aus Anhang A definiert. Die Prüfnachweise bzw. Herstellererklärungen zu den einzelnen Modulen sind der Zertifizierungsstelle im Rahmen des Zertifizierungsverfahrens vorzulegen.

Um die korrekte funktionale Implementierung der Module zu prüfen, werden funktionale Tests oder Konformitätstest durchgeführt.

Sofern der Leser ein sicherheitsrelevantes Modul unterstützt (Module ab A.4), so muss die Sicherheit durch eine Common-Criteria-Zertifizierung nach Anhang E nachgewiesen werden. Je nach Modul müssen zusätzlich spezielle Anforderungen erfüllt werden, z.B. eine Bestätigung nach Signaturgesetz. Die individuellen Ausprägungen (Bauform, PIN, Biometrie, Anzeigen usw.) bestimmen hierbei den Prüfumfang und -aufwand.

B.1 Schnittstelle zum Host-Rechner

Die Funktionsprüfungen stellen die Interoperabilität zwischen verschiedenen Chipkartenlesern sicher und testen Grundlagenanforderungen durch praktische Prüfungen. Die durchgeführten Funktionsprüfungen sind in einem Prüfbericht zu dokumentieren.

Die Prüfungen der Lesegeräte umfasst

- die Installation eines Chipkartenlesers einschließlich PC/SC-Treiber unter den Betriebssystemen gemäß der Liste aus A.1.3 und
- die Funktionsprüfung einschließlich PC/SC-Schnittstelle unter diesen Betriebssystemen.

Die durchzuführenden Prüfungen sind in Anhang C beschrieben und sind von einer vom BSI für Prüfungen nach [TR-03105] anerkannten Prüfstelle durchzuführen.

B.2 Kontaktlose Schnittstelle

Der Kartenleserhersteller hat im Rahmen der Prüfung darzustellen, dass eine Beschädigung von Chipkarten im Format td-1 (bis zu einer Dicke von 1100µm, vergleiche A.2) bei Nutzung der kontaktlosen Schnittstelle vermieden wird.

Für alle Lesertypen ist die Konformität zu [TR-03105], part 4, nachzuweisen. Hierzu ist eine Konformitätsprüfung der ISO Layer 2-4 bei einer vom BSI anerkannten Prüfstelle durchzuführen. Als Nachweis sind sämtliche Prüfberichte der Konformitätsprüfung vorzulegen.

B.3 Kontaktbehaftete Schnittstelle

Die kontaktbehaftete Schnittstelle muss nach [ISO 10373], part 3, geprüft werden. Die Prüfung ist von einer vom BSI gemäß DIN ISO/IEC 17025 anerkannten Prüfstelle durchzuführen. Ersatzweise können Prüfungen nach [EMV] zusammen mit Ergänzungsprüfungen nach [ISO 10373] durchgeführt werden. Der genaue Testumfang wird durch das BSI vorgegeben.

B.4 PIN-Pad mit PACE-Unterstützung

Zur Validierung der PACE-Implementierung ist eine Konformitätsprüfung der ISO Layer 6 und 7 gemäß [TR-03105], part 5.2, bei einer vom BSI anerkannten Prüfstelle durchzuführen. Es sind wenigstens die Profi-

le R_Tra, R_PACE und R_eID durchzuführen. Die in der Herstellererklärung (Implementation Conformance Statement, ICS) angegebenen Lesegerätfunktionen können die durchzuführenden Testfälle einschränken.

Als Nachweis sind sämtliche Prüfberichte der Konformitätsprüfung vorzulegen.

Die Einhaltung der Sicherheitsvorgaben, insbesondere

- Sicherer Umgang mit eingegeben PINs, insbesondere Löschen der PIN nach Nutzung.
- Sichere Implementierung von PACE (z.B. Schlüsselerzeugung)
- Einhaltung der Filterregeln
- Manipulationsschutz
- Sofern vorhanden: Anzeige des Sicherheitszustands

sind durch eine Common-Criteria-Zertifizierung nachzuweisen (siehe Anhang E).

B.5 Display

Die Sicherheit des Displays, insbesondere

- Authentische Anzeige, insbesondere korrekte Anzeige des Berechtigten und der Berechtigungen bei Nutzung der eID-Funktion
- Manipulationssicherheit der Anzeige

ist durch eine Common-Criteria-Zertifizierung nachzuweisen (siehe Anhang E).

B.6 QES mit kontaktbehafteten Karten

Es ist eine Bestätigung nach Signaturrecht von einer bei der Bundesnetzagentur anerkannten Prüfstelle vorzulegen.

B.7 QES mit kontaktlosen Karten gemäß TR-03117

Es ist eine Konformitätsprüfung der ISO Layer 6 und 7 gemäß [TR-03105], part 5.2, bei einer vom BSI anerkannten Prüfstelle durchzuführen. Es sind wenigstens die Profile R_Tra, R_PACE, R_TA, R_CA, R_eID und R_Sig durchzuführen. Die in der Herstellererklärung (Implementation Conformance Statement, ICS) angegebenen Lesegerätfunktionen können die durchzuführenden Testfälle einschränken.

Als Nachweis sind sämtliche Prüfberichte der Konformitätsprüfung vorzulegen.

Die Sicherheit der speziellen Mechanismen für die Nutzung der QES mit dem Personalausweis ist durch folgende Zertifizierungen nachzuweisen:

- Der private Schlüssel für die Terminalauthentisierung muss sicher gespeichert werden. Hierzu muss ein gemäß [PP-SSCD] nach Common Criteria mit Assurance Level EAL4+ zertifiziertes Sicherheitsmodul verwendet werden. In Ausnahmefällen können in Abstimmung mit dem BSI auch andere Sicherheitsmodule verwendet werden.
- Die auf das Sicherheitsmodul zugreifende Software (Firmware) muss mit Assurance Level EAL 3 zertifiziert sein. Dies geschieht auf Basis eines Security Targest des Hersteller. Empfohlen wird, dieses Security Target auf Basis des Protection Profiles [PP-IS] zu erstellen. Wird das Security Target nicht von diesem Protection Profile abgeleitet, so muss sichergestellt werden, dass die entsprechenden Sicherheitsanforderungen im Security Target abgebildet werden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

- Sofern der optionale Import eines neuen privaten Schlüssels für die Terminalauthentisierung implementiert wird, so muss der Importmechanismus mit Assurance Level EAL4+ zertifiziert werden. Dies wird nicht durch [PP-IS] abgedeckt, muss also im Security Target zusätzlich berücksichtigt werden.

Es ist eine Bestätigung nach Signaturrecht von einer bei der Bundesnetzagentur anerkannten Prüfstelle vorzulegen.

B.8 Firmware-Update

Die Sicherheit des Firmware-Updates, insbesondere

- Integritätssicherung und -prüfung der Firmware

ist durch eine Common-Criteria-Zertifizierung nachzuweisen, sofern die Firmware sicherheitsrelevante Bestandteile enthält (siehe Anhang E).

C Funktionale Prüfung

Die Prüfungen in diesem Abschnitt testen die Funktionsfähigkeit der Kartenleser bzw. der zugehörigen Treibern unter den unterstützten Betriebssystemen (siehe Anhang A.1). Die funktionale Prüfung ersetzt nicht die Konformitätsprüfungen nach [TR-03105].

C.1 Generelle Anforderungen

Zur Durchführung der Funktionsprüfung von Lesegeräten sind gleich bleibende und reproduzierbare Testumgebungen zu schaffen. Die nachfolgenden Unterkapitel beschreiben die Anforderungen an die Prüfwerkzeuge sowie die notwendigen Vorbereitungen zur Durchführung der Tests.

C.1.1 Prüfwerkzeuge

Zur Durchführung der Prüfungen sind verschiedene Hardware- und Softwarekomponenten notwendig. Prinzipiell sollte der Prüfaufbau der Ausstattung eines Computers beim Heimanwender entsprechen.

- Betriebssysteme gemäß Anhang A.1, jeweils mit allen aktuellen Patches des Betriebssystemherstellers
- eingerichteter Internetzugang
- aktuelle Version der AusweisApp[5]
- nPA-Testkarte bzw. nPA-Simulator

C.1.2 Vorbereitung

Zur Durchführung der Tests ist jeweils ein eigenes Testsystem für jedes geforderte Betriebssystem aufzusetzen. Die Installation der verschiedenen Betriebssysteme in virtuellen Maschinen ist nicht zulässig, da die Anbindung des Kartenlesers größtenteils vom Hostsystem abhängt, welches die virtuelle Maschine betreibt.

Die Installationen der Windows und Linux-Betriebssysteme können jeweils auf der gleichen Hardwareplattform getestet werden. Für Prüfung unter dem Betriebssystem Mac OS muss die vom Hersteller geforderte Hardwareplattform verwendet werden.

Alle Betriebssysteme müssen vor der Durchführung der Tests durch vom Betriebssystem-Hersteller bereitgestellte Updates auf den aktuellsten Versionsstand aktualisiert werden.

Ebenso ist immer die aktuelle, offiziell zur Verfügung stehende AusweisApp (www.ausweisapp.bund.de) auf den Prüfrechnern zu installieren.

Zudem ist ein Browser für die Verwendung mit der AusweisApp einzurichten. Dazu ist ggf. die Installation eines Browserplugins notwendig.

Die Installation der Lesegerät-Treiber ist bereits Teil der Tests.

5 Quelle: https://www.ausweisapp.bund.de

C.2 Prüfungen

Alle hier aufgeführten Tests sind jeweils unter den im Anhang A.1 aufgeführten Betriebssystemen durchzuführen.

C.2.1 Installationstests

Die Installation des Lesegeräts erfolgt – sofern vorhanden – nach der vom Hersteller gelieferten Installationsanleitung. Liegt dem Leser keine Anleitung bei, erfolgt die Installation durch Anschließen des Lesegeräts und anschließender Installation des Gerätetreibers nach gängigen Installationsmethoden. Diese sind im Prüfbericht zu dokumentieren.

Das Lesegerät wird wie in der Installationsanweisung des Herstellers beschrieben an das Testsystem angeschlossen. Wird vor dem Anschluss des Lesegeräts die Installation einer Software (vom Lesegeräte-Hersteller bereitgestellt oder Fremdsoftware) gefordert, ist diese, wie vom Lesegeräte-Hersteller beschrieben, vorher zu installieren.

Wird das Lesegerät nach Anschluss an das Testsystem vom Betriebssystem automatisch als bekanntes Gerät erkannt, ist trotzdem der vom Hersteller empfohlene aktuelle Treiber zu installieren.

Fehler durch falsche, fehlende oder inkompatible Betriebssystemkomponenten (z.B. fehlende Paket-Abhängigkeiten bei Linux-Systemen) sind zu analysieren und dokumentieren.

C.2.2 Funktionstests

Für die nachfolgenden Tests ist ein erfolgreich installiertes Lesegerät erforderlich. Alle hier beschriebenen Tests haben das Ziel, die Funktionsfähigkeit des Lesegeräts im Zusammenspiel mit der AusweisApp zu überprüfen. Je nach verwendeten Modulen gemäß Anhang A unterscheidet sich die Durchführung der Tests geringfügig. Herstellerspezifische Zusatzsoftware wird nicht überprüft.

Statt einer Testkarte kann auch ein entsprechender Simulator für die Durchführung der Leser-Tests verwendet werden. Dadurch kann sich der Testaufwand minimieren, da der Zustand der Karte (suspended, blocked) direkt simuliert werden kann.

Bei Lesegeräten mit Display ist darauf zu achten, dass die angezeigten Meldungen aus Kapitel A.5 verwendet werden und mit den Funktionen des jeweiligen Tests übereinstimmen.

C.2.2.1 Kartenerkennung

Nach Auflegen der Testkarte auf den zu testenden Leser wird das Erkennen der Karte durch die AusweisApp kenntlich gemacht.

Vorbereitung

- Keine Vorbereitung erforderlich

Durchführung

- Die Karte wird in die vom Hersteller vorgesehene Lesepostion des Lesers platziert.

Dokumentation

- Es ist zu dokumentieren, ob die Karte erkannt wurde und in der AusweisApp angezeigt wurde.

C.2.2.2 Leserinformationen

Es wird überprüft ob der Kartenleser das Auslesen der Leserinformationen (siehe Kapitel A.1.2) unterstützt.

Vorbereitung

- Keine Vorbereitung erforderlich

Durchführung

- Nacheinander folgend sind alle vier Kommandos aus Kapitel A.1.2 Tabelle 3 an das Lesegerät zu senden. In der Antwort werden die abgefragten Informationen im String-Format sowie das Statuswort 0x9000 erwartet.

Dokumentation

- Es sind alle Rückgabewerte zu dokumentieren.

C.2.2.3 PIN-Änderung

Mithilfe der AusweisApp ist die PIN der Testkarte zu ändern.

Bei einem Lesegerät ohne PIN-Pad ist die PIN auf Aufforderung über die Tastatur des Prüfrechners einzugeben.

Bei einem Lesegerät mit PIN-Pad muss die PIN über dieses eingegeben werden. Eine Eingabeaufforderung für die PIN über die PC-Tastatur ist bei diesen Lesergeräten nicht zulässig. Sollte die PIN-Eingabeaufforderung auf dem Prüfrechner erscheinen, ist die PIN trotzdem nur auf dem PIN-Pad des zu testenden Lesegeräts einzugeben. Eine Rückkopplung der am PIN-Pad eingegebenen PIN zum Prüfrechner ist nicht zulässig.

Bei Lesegeräten mit einem Display muss die Aufforderung zur PIN-Eingabe am Leser angezeigt werden.

Vorbereitung

- Die Karte wird in die vom Hersteller vorgegebene Lesepostion gebracht.

Durchführung

- In der AusweisApp wird die PIN-Änderung aufgerufen.
- Die PIN wird auf einen neuen Wert gesetzt.
- Nach erfolgreicher Änderung ist die PIN wieder in den ursprünglichen Wert zu ändern.

Dokumentation:

- Die Rückmeldung über beide Änderungen der PIN ist zu dokumentieren.
- Zudem ist zu dokumentieren, ob die PIN-Eingabe über die PC-Tastatur oder das PIN-Pad des Lesegeräts erfolgte.

C.2.2.4 CAN-Eingabe

Die Karte ist in den Zustand "suspended" (siehe [TR-03110]) zu bringen. Das Lesegerät bzw. die AusweisApp müssen daraufhin zur Eingabe der CAN auffordern.

Beim Standard- bzw. Komfortleser muss die PIN über das PIN-Pad des Lesegeräts eingegeben werden. Eine Eingabeaufforderung für die PIN über die PC-Tastatur ist bei diesen Lesertypen nicht zulässig.

Bei Lesegeräten mit einem Display sollte die Aufforderung zur PIN und CAN-Eingabe am Leser angezeigt werden.

Vorbereitung

- Die Karte wird in die vom Hersteller vorgegebene Lesepostion gebracht.
- Die Karte wird in den Zustand "suspended" (siehe [TR-03110]) gebracht.
  Eine mögliche Vorgehensweise: In der AusweisApp wird der Punkt PIN-Änderung aufgerufen. Die PIN wird solange wiederholt falsch eingegeben, bis die Eingabe der CAN gefordert wird.
  Alternativ kann ein Simulator eingesetzt werden, der diesen Zustand direkt simuliert.

Durchführung

- Die korrekte CAN wird eingegeben. Falls die AusweisApp die Eingabe der CAN direkt in der Applikation auch bei Lesegeräten mit eigenem PIN-Pad anbietet, soll die Eingabe der CAN sowohl per PIN-Pad als auch über die AusweisApp getestet werden.
- Die korrekte PIN wird eingegeben. Die PIN-Eingabe darf bei Lesegeräten mit eigenem PIN-Pad nur direkt am Lesegerät möglich sein.

Dokumentation

- Die Aufforderung zur Eingabe der CAN und der PIN sowie die Rückmeldung des Lesegeräts und der AusweisApp sind zu dokumentieren.
- Zudem ist zu dokumentieren, ob die PIN- bzw. CAN-Eingabe über die AusweisApp oder das PIN-Pad des Lesegeräts erfolgte.

C.2.2.5 PUK-Eingabe

Die Karte ist in den Zustand „blocked" (siehe [TR-03110]) zu bringen. Anschließend ist das korrekte Verhalten zur Abfrage und Eingabe der PUK des Lesegeräts zu überprüfen.

Bei Lesegeräten mit eigenem PIN-Pad muss die PIN und PUK über das PIN-Pad des Lesegeräts eingegeben werden. Eine Eingabeaufforderung für die PIN oder PUK über die PC-Tastatur ist bei diesen Lesertypen nicht zulässig.

Bei Lesegeräten mit einem Display muss die Aufforderung zur PIN, CAN bzw. PUK-Eingabe am Leser angezeigt werden.

Vorbereitung

- Die Karte wird in die vom Hersteller vorgegebene Lesepostion gebracht.
- Die Karte ist in den Zustand "blocked" (siehe [TR-03110]) zu bringen.
  Eine mögliche Vorgehensweise: In der AusweisApp wird die PIN-Änderung aufgerufen. Die PIN wird durch mehrmalige Falscheingabe in den Zustand "suspended" gebracht. Es wird die korrekte CAN und anschließend erneut eine falsche PIN eingegeben. Die Karte ist nun im Zustand "blocked".
  Alternativ kann ein Simulator eingesetzt werden, der diesen Zustand direkt simuliert.

Durchführung

- Zum Entsperren der Karte ist die entsprechende Funktion in der AusweisApp aufzurufen. Nach Eingabe der korrekten PUK ist die ursprüngliche PIN wieder aktiv.

Dokumentation

- Die Anzeige, das Eingabeverfahren und die Rückmeldung des Lesegeräts sowie der AusweisApp, sind zu dokumentieren.

C.2.2.6 Online-Authentisierung

Bei dieser Prüfung ist eine komplette Authentisierung an einem Online-Portal durchzuführen.

Bei Lesegeräten mit PIN-Pad muss die PIN über das PIN-Pad des Lesegeräts eingegeben werden. Eine Eingabeaufforderung für die PIN über die PC-Tastatur ist bei diesen Lesertypen nicht zulässig.

Bei Lesegeräten mit einem Display sollte die Aufforderung zur PIN-Eingabe am Leser angezeigt werden. Ebenso sollte das Display die Daten des Berechtigungszertifikates Anzeigen.

Vorbereitung

- Die Karte wird in die vom Hersteller vorgegebene Lesepostion gebracht.
- Im Browser wird die Anmeldeseite eines Diensteanbieters mit nPA-Anmeldung aufgerufen.

Durchführung

- Auf dem Dienstportal wird die Anmeldung gestartet.
- Bei Lesegeräten mit Display müssen die Daten im Display mit denen des in der AusweisApp angezeigten Daten aus dem Berechtigungszertifikat übereinstimmen.
- Die Anmeldeprozedur wird durchlaufen und mit der Eingabe der korrekten PIN authentisiert. Die PIN-Eingabe darf bei Lesegeräten mit eigenem PIN-Pad nur direkt am Lesergerät möglich sein. Nur bei Lesegeräten ohne eigenes PIN-Pad ist die Eingabe der PIN über die AusweisApp zulässig.
- Die erfolgreiche Anmeldung wird innerhalb des Portals durch Kontrolle der freigegebenen Daten überprüft.

Dokumentation

- Das verwendete Dienstportal ist zu dokumentieren.
- Die Anzeige, das Eingabeverfahren und die Rückmeldung des Lesegeräts sowie der AusweisApp, sind zu dokumentieren.
- Die Rückmeldung des Dienstportals nach der Anmeldeprozedur ist zu dokumentieren.

C.3 Prüfprotokoll

Das Prüfprotokoll muss mindestens folgende Angaben enthalten:

- Firmen und Typbezeichnung des Lesegerätes
- Firmware-Version des Lesegerätes
- Treiber-Version des Lesegerätes
- Verwendete Betriebssysteme und Versionsstand der installierten Patches (Service-Packs, Kernel-Versionen, PCSC-Dämon)
- Versionsnummer der AusweisApp
- Verwendete Testkarte bzw. Simulator
- Verwendetes Dienstanbieterportal
- Ergebnisse der beschriebenen Prüfungen
- Abweichungen von den beschriebenen Prüfanweisungen sind detailliert zu beschreiben und zu begründen. Abschließend ist eine Gesamtbeurteilung der Funktionsfähigkeit des getesteten nPA-Lesegerätes durch die Prüfstelle zu erstellen.

D PC/SC-Erweiterung

Sofern ein Kartenleser eines der Module A.4, A.5 oder A.7 implementiert, muss dieser zur Unterstützung von PACE und EAC nach [TR-03110] und [TR-03117] das hier definierte PC/SC-Feature FEATURE_EXECUTE_PACE unterstützen. Das Feature umfasst die Funktionen GetReaderPACECapabilities und EstablishPACEChannel.

In den Definitionen werden die Datentypen BYTE (unsigned 8 bit), USHORT (unsigned 16 bit) und DWORD (unsigned 32 bit) nach [PC/SC], part 9, verwendet. BYTE[] bezeichnet ein Array von BYTEs.

D.1 FEATURE_EXECUTE_PACE

Die in [PC/SC], part 10, spezifizierte Funktion GET_FEATURE_REQUEST wird erweitert um FEATURE_EXECUTE_PACE mit dem numerischen Wert 0x20. Der damit ermittelte Controlcode CTRL_FEATURE_EXECUTE_PACE wird dann mit SCardControl für alle PACE-Funktionen verwendet.

D.1.1 SCardControl

- InBuffer:

Position	*Länge in Bytes, Type*	*Name*	*Beschreibung*
1	1, BYTE	idxFunction	Index der PACE-Funktionen
2	2, USHORT	lengthInputData	Größe von Pos. 3
3	lengthInputData, BYTE[]	InputData	Funktionsabhängige Eingabedaten

- Funktionsindizes:

Index	*Funktion*
1	GetReaderPACECapabilities
2	EstablishPACEChannel

- OutBuffer:

Position	*Länge in Bytes, Type*	*Name*	*Beschreibung*
1	4, RESPONSECODE	Result	Ergebniscode
2	2, USHORT	lengthOutputData	Größe von Pos. 3
3	lengthOutputData, BYTE[]	OutputData	Funktionsabhängige Ausgabedaten

- Ergebniscodes:

Code	*Beschreibung*

0x00000000	Kein Fehler
Fehler in den Input-Daten	
0xD0000001	Längen im Input sind inkonsistent
0xD0000002	Unerwartete Daten im Input
0xD0000003	Unerwartete Kombination von Daten im Input
Fehler im Protokollablauf	
0xE0000001	Syntaxfehler im Aufbau der TLV-Antwortdaten
0xE0000002	Unerwartete/fehlende Objekte in den TLV-Antwortdaten
0xE0000003	Der Kartenleser kennt die PIN-ID nicht.
0xE0000006	Fehlerhaftes PACE-Token
0xE0000007	Zertifikatskette für Terminalauthentisierung kann nicht gebildet werden
0xE0000008	Unerwartete Datenstruktur in Rückgabe der Chipauthentisierung
0xE0000009	Passive Authentisierung fehlgeschlagen
0xE000000A	Fehlerhaftes Chipauthentisierung-Token
Vom PCD erzeugte APDU für PACE liefert Fehler (Statuswort SW1SW2)	
0xF000SW1SW2	Select EF.CardAccess
0xF001SW1SW2	Read Binary EF.CardAccess
0xF002SW1SW2	MSE: Set AT für PACE
0xF003SW1SW2 – 0xF006SW1SW2	General Authenticate Step 1-4
Vom PCD erzeugte APDU für Terminal-/Chipauthentisierung liefert Fehler (Statuswort SW1SW2)	
0xF800SW1SW2	MSE: Set DST (erstes Zertifikat)
0xF801SW1SW2	PSO: Verify Certificate (erstes Zertifikat)
0xF802SW1SW2	MSE: Set DST (zweites Zertifikat)
0xF803SW1SW2	PSO: Verify Certificate (zweites Zertifikat)
0xF804SW1SW2	MSE: Set DST (drittes Zertifikat)
0xF805SW1SW2	PSO: Verify Certificate (drittes Zertifikat)
0xF806SW1SW2	MSE: Set AT für Terminalauthentisierung
0xF807SW1SW2	Get Challenge
0xF808SW1SW2	External Authenticate
0xF809SW1SW2	Select EF.CardSecurity
0xF80ASW1SW2	Read Binary EF.CardSecurity
0xF80BSW1SW2	MSE: Set AT für Chipauthentisierung
0xF80CSW1SW2	General Authenticate
Sonstige Fehler	
0xF0100001	Kommunikationsabbruch mit Karte.

0xF0100002	Keine Karte im Feld.
0xF0200001	Benutzerabbruch.
0xF0200002	Benutzer-Timeout

D.2 GetReaderPACECapabilities

Für die Unterstützung von PACE und EAC werden folgende Capabilities definiert:

- **PACE (0x40)**: Der Leser kann PACE durchführen
- **eID (0x20)**: Der Leser unterstützt die eID-Funktion und, sofern der Kartenleser ein Display besitzt, die Anzeige von eID-Daten aus dem Berechtigungszertifikat
- **eSign (0x10)**: Der Leser unterstützt die QES mit kontaktlosen Karten nach [TR-03117].

Mittels der Funktion GetReaderPACECapabilities wird festgestellt, welche der Capabilities vom Leser unterstützt werden.

- InputData: Keine
- OutputData:

Position	*Länge in Bytes*	*Name*	*Beschreibung*

1	1, BYTE	lengthBitMap	Größe von Pos. 2
2	lengthBitMap, BYTE[]	BitMap	Capabilities

D.3 EstablishPACEChannel

Die Funktion EstablishPACEChannel dient zum Aufbau des PACE-Kanals sowie ggfs. der Anzeige von eID-Informationen bzw. Authentisierung eines Signaturterminals. Im Folgenden wird der Ablauf der Funktion EstablishPACEChannel beschrieben. Abbildung 2 gibt einen Überblick über die einzelnen Schritte.

1. Der Host-Rechner ruft EstablishPACEChannel auf.
2. Der Kartenleser liest das EF.CardAccess der Karte und extrahiert die für das PACE-Verfahren notwendigen Parameter.
3. Der Kartenleser extrahiert aus InputData
   - die PIN-ID (PIN, CAN, MRZ, PUK)
   - und – sofern vorhanden – den CHAT (Certificate Holder Authorization Template).
4. Entsprechend der Rolle des Terminals wird das PACE-Protokoll eingeleitet:
   - MSE: Set AT
   - General Authenticate Step 1+2

Chip	*Kartenleser*	*Host-Rechner*
	Aufruf von EstablishPACEChannel	
Extrahieren der für PACE notwendigen Parameter aus EF.CardAccess		
	PIN-ID aus InputData Prüfung auf Rolle des Terminals	
MSE: Set AT General Authenticate Step 1+2		
	Bei Nutzung Capability eID: Extrahieren und Anzeigen Berechtigter aus InputData Anzeige der Berechtigungen aus CHAT Berechnung der Variablen StoreHash	
	Eingabe der PIN Berechnung Kπ Entschlüsselung 'Encrypted Nonce' mit Kπ Bereinigen des Speichers	
General Authenticate Step 3+4 Berechnung des Schlüsselmaterials für Secure Messaging		
	Bei Nutzung Capability eID: Bei ‚PSO: Verify Certificate' Vergleich Hash aus Certfica-te Extensions mit Variable StoreHash	
Bei Nutzung Capability eSign: Durchführung von Terminalauthentisierung, Passiver Authentisierung und Chipauthen-tisierung, Restart des Secure Messaging		

Abbildung 2: Ablauf PACE

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

5. Bei Nutzung der Capability eID und Vorhandensein eines Displays: Der Kartenleser extrahiert aus InputData die Zertifikatsbeschreibung, extrahiert daraus den Berechtigten und bringt diesen zur Anzeige. Sollte es keine Zertifikatsbeschreibung geben oder der Berechtigte kann mit dem Zeichensatz des Kartenlesers nicht dargestellt werden, wird als Berechtigter ‚Unbekannt' angezeigt. Danach werden die im CHAT enthaltenen Berechtigungen zur Anzeige gebracht. Der Anwender kann diese am Leser einzeln überprüfen, jedoch keine weiteren Einschränkungen mehr vornehmen.Der Leser berechnet den Hash über die Zertifikatsbeschreibung und speichert diesen.
6. Der Kartenleser fordert (sofern nicht in den InputData enthalten) zur Passwort-Eingabe auf und leitet danach K_π ab. Werden als Passwort PIN oder PUK verwendet, so muss das Passwort am PIN-Pad eingegeben werden. Der Kartenleser entschlüsselt die „Encrypted Nonce" mit K_π. Der Kartenleser bereinigt den Speicher von Informationen, die Rückschlüsse auf die PIN zulassen.
7. Der Kartenleser führt die restlichen Schritte General Authenticate Step 3+4 durch und bildet das Schlüsselmaterial für das Secure Messaging zwischen Kartenleser und Chip.
8. Bei Nutzung der Capability eID und Vorhandensein eines Displays: Alle Befehle, für die der Kartenleser das Secure Messaging durchführt, werden überwacht und bei allen ‚PSO:Verify Certificate' werden, wenn es sich um das Terminalzertifikat handelt, die Certificate Extensions extrahiert und der darin ggf. enthaltenen Hash-Wert mit dem in Schritt 5 gespeicherten Wert verglichen. Sind diese beiden Werte unterschiedlich, wird der Befehl geblockt und als Antwort SW1SW2 wird 69 85 zurückgegeben.
9. Bei Nutzung der Capability eSign: Das Kartenleser führt im Anschluss an den Aufbau des PACE-Kanals direkt die Terminalauthentisierung und die Chipauthentisierung durch. Nach erfolgreicher Durchführung der Chipauthentisierung wird das Secure Messaging mit PACE-Schlüsseln beendet und durch Secure Messaging mit den neu ausgehandelten Schlüsseln abgelöst.

Ein- und Ausgabedaten des Aufrufs EstablishPACEChannel sind wie folgt definiert:

- InputData:

Position	*Länge in Bytes*	*Name*	*Beschreibung*
1	1, BYTE	PinID	0x01: MRZ 0x02: CAN 0x03: PIN 0x04: PUK
2	1, BYTE	lengthCHAT	Größe von Pos. 3
3	lengthCHAT, BYTE[]	CHAT	Das eingeschränkte CHAT für das Terminalzertifikat
4	1, BYTE	lengthPIN	Größe von Pos.5
5	lengthPIN, BYTE[]	PIN	Passwort kann vom Host vorgegeben werden, z.B. gespeicherte CAN
6	2, USHORT	lengthCertificateDescription	Größe von Pos. 7
7	lengthCertificateDescription, BYTE[]	CertificateDescription	Komplette Zertifikatsbeschreibung,so, dass der Kartenleser den Hash berechnen kann.

Für eine Durchführung von PACE in der Rolle

- eines nicht-authentisierten Terminals (Capability PACE) ist nur die Position 1 vorhanden
- in der Rolle Authentisierungsterminal (Capability eID) sind alle Positionen anzugeben

- in der Rolle Signaturterminal (Capability QES) sind die Positionen 1-3 und ggfs. 4-5 (für Passwort CAN, sofern dieses nicht am Leser eingegeben wird) anzugeben.

- OutputData:

Position	*Länge in Bytes*	*Name*	*Beschreibung*
1	2, USHORT	Statusbytes	Statusbytes bei Antwort auf MSE:Set AT
2	2, USHORT	lengthEF_CardAccess	Größe von Pos. 3
3	lengthEF_CardAccess, , BYTE[]	EF_CardAccess	Inhalt von EF.CardAccess
4	1, BYTE	lengthCAR	Größe von Pos. 5
5	lengthCAR, BYTE[]	CAR	Aktuelle Certificate Authority Reference
6	1, BYTE	lengthCARprev	Größe von Pos. 7
7	lengthCARprev, BYTE[]	CARprev	Vorangegangene Certificate Authority Reference
8	2, USHORT	length_IDicc	Größe von Pos. 9
9	length_IDicc, BYTE[]	IDicc	IDicc ist für spätere Terminalauthentisierung notwendig

Positionen 4-9 sind nur bei einer Durchführung von PACE in der Rolle eines Authentisierungsterminals vorhanden. Im Fehlerfalle werden keine Daten zurückgegeben.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 4. August 2011
Fundstelle: eBAnz AT101 2011 B1
– veröffentlicht am 31. August 2011 –
Quelle: elektronischer Bundesanzeiger

E IT-Sicherheitsevaluierung

Die Erfüllung der an den Chipkartenleser gestellten IT-Sicherheitsanforderungen ist durch eine IT-Sicherheitsevaluierung und -zertifizierung gemäß den Common Criteria (Common Criteria for Information Technology Security Evaluation, Version 3.1) nachzuweisen. Für Chipkartenleser ohne QES-Unterstützung ist hier die Prüfstufe EAL3, für Chipkartenleser mit QES-Unterstützung die Prüfstufe EAL3+ anzuwenden.

Die IT-Sicherheitsevaluierung ist von einer vom BSI gemäß DIN ISO/IEC 17025 anerkannten Prüfstelle durchzuführen. Die anschließende IT-Sicherheitszertifizierung erfolgt durch das BSI.

Als zentrale Grundlage für die IT-Sicherheitsevaluierung dient ein sog. Security Target (ST). Das ST wird vom Hersteller des Chipkartenlesers erstellt und muss je nach dessen Ausprägung folgende Mindestsicherheitsanforderungen/-funktionen abdecken:

- Sicherer Umgang mit eingegeben PINs, insbesondere Löschen der PIN nach Nutzung (Modul A.4).
- Sichere Implementierung von PACE (z.B. Schlüsselerzeugung) (Modul A.4)
- Einhaltung der Filterregeln (Modul A.4)
- Sofern vorhanden: Anzeige des Sicherheitszustands (Modul A.4)
- Authentische Anzeige, insbesondere korrekte Anzeige des Berechtigten und der Berechtigungen bei Nutzung der eID-Funktion (Modul A.5)
- Manipulationssicherheit (Modul A.4, A.5)
- Integritätssicherung und -prüfung der Firmware (Modul A.8)

Unterstützt der Chipkartenleser verschiedene Applikationen oder verschiedene Sicherheitsmodi, so ist die Abgrenzung der Applikationen und die sichere Trennung der Sicherheitsmodi ebenfalls Bestandteil des Security Targets.

Unterstützt der Chipkartenleser die qualifizierte Signatur, so sind die Sicherheitsanforderungen des Signaturrechtes im Security Target zu berücksichtigen. Bei Unterstützung der QES mit dem Personalausweis sind die besonderen Prüfanforderungen aus B.7 zu berücksichtigen.

Literaturverzeichnis

[AIS 20]	BSI: AIS 20 -- Functionality classes and evaluation methodology for deterministic random number generators.
[CP-eSign]	BSI: Certificate Policy für die eSign-Anwendung des ePA
[PP-IS]	BSI: Common Criteria Protection Profile for Inspection Systems, BSI-CC-PP-0064
[TR-03105]	BSI: Technische Richtlinie TR-03105, Conformity Tests for Official Electronic ID Documents
[TR-03110]	BSI: Technische Richtlinie TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE) and Restricted Identification (RI), Version 2
[TR-03116]	BSI: Technische Richtlinie TR-03116, Technische Richtlinie für die eCard-Projekte der Bundesregierung
[TR-03117]	BSI: Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit
[CEN 1332]	CEN: prEN 1332-5 - Identification card systems – Man machine interface – Part 5: Raised tactile symbols for differentiation of application on ID-1 cards
[PP-SSCD]	CEN: prEN 14169-1 -- Protection Profile for Secure signature creation device -- Part 2: Device with key generation, BSI-CC-PP-0059
[EMV]	EMV: Integrated circuit card, Specification for Payment systems, Application independent ICC to terminal interface requirements
[ICAO 9303]	ICAO: Doc 9303, Machine Readable Travel Documents, Part 3
[ISO 14443]	ISO/IEC: ISO 14443 - Identification cards – Contactless integrated circuit(s) cards – Proximity cards
[ISO 7810]	ISO/IEC: ISO 7810 - Identification cards - Physical characteristics
[ISO 7816]	ISO/IEC: ISO 7816 - Identification cards – Integrated circuit cards
[ISO 10373]	ISO/IEC: ISO/IEC 10373 -- Identification cards -- Test methods
[PC/SC]	PC/SC Workgroup: PC/SC Workgroup Specifications 1.0/2.0
[CT-API]	TeleTrust: CT-API – Anwendungsunabhängiges CardTerminal Application Programming Interface für Chipkartenanwendungen
[MKT]	TeleTrust: Multifunktionale KartenTerminals MKT-Spezifikation – MKT-Version 1.0