Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03119

Anforderungen an Chipkartenleser mit ePA Unterstützung

Version 1.1

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0

Internet: https://www.bsi.bund.de

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Inhalt

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Tabellenverzeichnis

Abbildungsverzeichnis

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.

Der elektronische Personalausweis (ePA) ist eine Komponente für derartige neue Prozesse, die ohne Medienbrüche zu einer schnellen und gesicherten Personenidentifikation und -authentifikation beitragen sollen.

Der ePA soll neben dem Einsatz in hoheitlichen Anwendungen über eGovernment auch Anwendungen der privatwirtschaftlichen Industrie und Banken unterstützen.

Hierzu werden hohe Anforderungen an Funktionalität und Sicherheit von Chipkartenlesern gestellt.

Zum Schutz der Information, zur Wahrung der Vertraulichkeit, der Integrität und der Verfügbarkeit müssen sichere IT-Produkte eingesetzt werden.

Diese Spezifikation dient als Richtlinie bei der Entwicklung von multifunktionalen, interoperablen und sicheren Chipkartenlesern mit ePA Unterstützung und deren Anwendungen.

1 Einführung

Derzeitige Chipkartenleser eignen sich oft nur für einzelne oder standardisierte Anwendungen. So gibt es Geldkarten-Leser für das Bezahlen im Internet, KVK, MKT, SICCT und eHealth Kartenterminals für das Gesundheitswesen, Signaturkartenleser für eine gesetzeskonforme Signatur, B1 Chipkartenleser für Company Card Anwendungen und viele andere, untereinander inkompatible, Lösungen.

Es ist angedacht, in dieser Technischen Richtlinie eine möglichst kompatible und interoperable Basis zu schaffen, die untereinander kompatible Chipkartenleser erwirkt, die zudem in möglichst vielen weiteren Anwendungen eingesetzt werden können.

Hierbei soll es auch dem Anwendungsprogrammierer möglich sein, auf eine einheitliche Schnittstelle aufsetzen zu können, die es erlaubt, zur Technischen Richtlinie konforme Chipkartenleser beliebiger Herkunft verwenden zu können.

Zwar gibt es beim ePA direkte Verwandtschaften zum elektronischen Reisepass (ePassport), jedoch erfordern zum Beispiel qualifizierte elektronische Signaturen (QES) und geplante privatwirtschafliche Anwendungen besondere Anforderungen an die Ausprägungen des Chipkartenlesers. Berücksichtigt werden jedoch kompatible Ansätze aus nationalen und internationalen Standards, Regelwerken und Richtlinien sowie nicht zuletzt die ausgearbeiteten Strategien des Bundes.

Diese Technische Richtlinie für kontaktbehaftete und kontaktlose Chipkartenleser gilt vorrangig für Geräte zur Verwendung des elektronischen Personalausweises und für weitere Kartenprojekte des Bundes mit denen privatwirtschaftliche Anwendungen genutzt werden können.

Die wichtigste Anforderung an einen Chipkartenleser ist der fehlerfreie, störungsfreie und zuverlässig Betrieb, und die Unversehrtheit der Chipkarten. Dazu sind bei kontaktlosen und kontaktbehafteten Chipkartenlesern weitere Anforderungen und Funktionen für interoperable Ziele notwendig.

Nicht minder wichtig ist die Berücksichtigung der Informationssicherheit um die Vertraulichkeit und Integrität der Abläufe und Kommunikationen gewährleisten zu können.

Da ein hoheitlicher Ausweisleser bei einer Personenidentifikation durch die Exekutive andere Merkmale besitzen muss, als ein Chipkartenleser für eine elektronische Signatur, werden diese Ausweisleser in dieser TR nicht berücksichtig. In diesem Dokument werden jedoch modulare Prozesse beschreiben, wonach für einzelne „Use Cases“ und deren speziellen Anforderungen die einzelnen Module zusammengestellt werden können und eine definierte Kategorie von Chipkartenlesern darstellen.

Durch obligatorische und optionale Kombinationen der Module ergeben sich konkrete Leserausprägungen, die in einzelnen Kapiteln dieser Technischen Richtlinie spezifiziert sind.

Diese Technische Richtlinie richtet sich an Entwickler und Hersteller von Chipkartenlesern sowie an Applikationsentwickler. Sie soll die Basis für eine Produktentwicklung, Tests, Einbindung und Nutzung von Chipkartenlesern für den ePA im kommerziellen und privaten Umfeld sein.

Die Technische Richtlinie stellt somit eine Zertifizierungsgrundlage dar.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

1.1 Abkürzungen

APDU	Application Protocol Data Unit
API	Application Programming Interface
BCS	Basic Command Set
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CE	Conformité Européenne
CEN	Comité Européen de Normalisation
CT	Card Terminal
CT-API	Card Terminal Application Programming Interface
DIN	Deutsches Institut für Normung
DIF	Deutsches Industrieforum
EAL	Evaluation Assurance Level
EN	Europäische Norm
EMV	Europay Mastercard Visa
ePA	Elektronischer Personalausweis
FinTS	Financial Transaction Services
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
IFD	Interface Device
ISO	International Standardization Organization
IT	Informationstechnik
KVG	Krankenversichertenkarte
MKT	Multifunktionales Kartenterminal
NFC	Near Field Communication
ÖPNV	Öffentlicher Personennahverkehr
PCD	Proximity Coupling Device
PC/SC	Personal Computer / Smartcard
PDA	Personal Digital Assistant
PICC	Proximity Integrated Circuit Card
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure

QES	Qualifizierte Elektronische Signatur
RFID	Radio Frequency Identification
RFU	Reserved for Future Use
SigG	Signaturgesetz
SICCT	Secure Interoperable Chipcard Terminal
TCP/IP	Transmission Control Protocol over Internet Protocol
TR	Technische Richtlinie
USB	Universal Serial Bus
UID	Unique Identification
VDV	Verband Deutscher Verkehrsunternehmen
WHQL	Windows Hardware Quality Labs

1.2 Terminologie

In tabellarischen Profilen werden die folgenden Abkürzungen verwendet:

- X: die Implementierung ist obligatorisch.
- O: die Implementierung ist optional.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

2 Interoperable ePA Chipkartenleser

Die geplanten Anwendungen für den ePA beschränken sich nicht nur auf den hoheitlichen Bereich. Vielmehr ist auch die privatwirtschaftliche Nutzung des ePAs beabsichtigt. In weiteren Anwendungen kann die NFC-Fähigkeit des ePAs unterstützt werden.

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

Alle beschriebenen Chipkartenleser sind primär für den ePA mit kontaktloser Kartenschnittstelle ausgelegt. Auch die kontaktbehaftete Schnittstelle ist mit berücksichtigt. Nach der Einführung grundlegender Eigenschaften und Anforderungen, werden ab Kapitel 3 ausgesuchte Chipkartenleser 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 Chipkartleser, der im Wesentlichen für die Kommunikation zwischen Chipkarte und Host verantwortlich ist, und einem Kartenterminal mit erweiterten Funktionen ist fließend.

In dieser TR wird anfangs nicht explizit zwischen Chipkartenleser und Kartenterminal unterschieden.

Es wird zunächst, unabhängig von den tatsächlichen Ausprägungen, von einem **Chipkartenleser** gesprochen. Je nach Anwendungsgebiet und den später genauer definierten „Use Cases“ werden die Ausprägungen jedoch wieder etwas genauer unterschieden, sowie falls notwendig spezielle Ausdrücke wie „Lesermodul“, Kartenterminal und PCD verwendet.

2.2 Architektur

Die Architektur der hier beschriebenen Chipkartenleser basiert, unter Berücksichtigung existierender Konzepte aus der Telekommunikation, des Gesundheitswesens und dem ePassport-Konzept, auf Grundlage der ICAO-Richtlinien.

Die Ansteuerung der Chipkarte, des Lesers und auch deren funktionalen Komponenten (Tastatur, Display, usw.) erfolgt über bytesequenzielle Kommandos in Form einer APDU Byte-Folge nach ISO/IEC 7816-4 [ISO4].

Bei der Ansteuerung durch einen Personalcomputer bieten sich weitere Vereinfachungen durch die Verwendung homogener Programmierschnittstellen an (API).

Neben Programmierschnittstellen wie CT-API [CT-API] oder PC/SC, bietet insbesondere das „eCard-API-Framework“ eine interoperable High-Level Programmierschnittstelle. Ist diese High

Level Programmierschnittstelle zur gewünschten Anwendung vorhanden, so werden die darunter liegenden Layer integriert und sind für den Programmierer nicht zwangläufig sichtbar.

2.3 Modulkonzept

Aufgrund der Chipkartenleservielfalt 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. Diese Module sind aufgrund definierter Schnittstellen, die auf internationale Normen oder branchenüblichen Standardwerken beruhen, beliebig kombinierbar und einzeln prüfbar.

Ist es bei Chipkartenlesern für Personalcomputer 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. Die Anforderungen an derartige Leser werden in einer folgenden Version der TR beschrieben.

Chipkartenleser für eine qualifizierte elektronische Signatur müssen zusätzlich weitere sicherheitsrelevante Eigenschaften unterstützten und bedürfen der Veröffentlichung als geeignete Komponente durch die Bundesnetzagentur.

Eine wichtige Anforderung der Informationssicherheit ist der Schutz vor unbefugter Preisgabe oder Veränderung von Daten. Je nach Einsatzgebiet ist es zum Beispiel erforderlich, dass der Chipkartenleser PIN-Eingaben intern verarbeitet.

Wenn nicht durch eine spezielle Leserausprägung ein Modul vorgeschrieben wird, sind die Module **optional** zu verwenden. 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 umgezusetzt werden. Ab Kapitel 3 werden speziellen Leserausprägungen dargestellt, die sich aus den Anforderungen der einzelnen Anwendungen (Use Cases) ergeben.

Die Module werden im Anhang A detailliert beschrieben.

2.4 Zertifizierung

Prüfstellen sind vom BSI akkreditierte Institutionen.

Die Prüfungen bestätigen, dass das Produkt, in Relation zu den implementierten Funktionen, die in den Produktbeschreibung angeführt sind, den Anforderungen dieser TR entspricht. Die Bestätigung bezieht sich auf Aspekte der Sicherheit, der Funktion und der Zuverlässigkeit.

Dadurch wird eine Konformität erreicht, die es erlaubt, Merkmale für die Verwendung abzufassen und interoperable Eigenschaften zu verwirklichen.

Ab Kapitel 3 sind zu den einzelnen Terminalvariationen konkrete Anforderungen beschrieben worden. Diese Anforderungen bilden die Basis für Prüfungen.

Die zu den Terminalvariationen gehörenden Kapitel für Nachweise und Prüfungen legen den Umfang der Prüfungen fest.

Wenn andere Spezifikationen (z.B. B1) in das Gerät implementiert wurden, muss auch hierfür ein entsprechender Prüfnachweis erbracht werden. Alle Prüfungen und die Ergebnisse müssen protokolliert werden und auf Anfrage jederzeit verifizierbar sein.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Ist kein Änderungsmanagement vorhanden und ist dieses Teil nicht der Zertifizierung gewesen, so müssen alle system- und funktionsrelevanten Änderungen dem BSI angezeigt werden.

Das BSI beschließt aufgrund der Änderungen, ob die Zertifizierung weiterhin gültig ist oder ob eine Delta- oder Neuzertifizierung erforderlich ist.
Als Nachweis der Zertifizierung erhält das Gerät ein vom BSI definiertes Qualitätssiegel, welches die Konformität des Gerätes zur TR-03119 dokumentiert.

2.4.1 Zertifizierungsverfahren

1. Antrag auf Zertifizierung beim BSI mit Benennung der Prüfstelle und Übergabe einer Produktbeschreibung.
2. Durchführung und Einreichen der Teilprüfungen bei der Prüfstelle.
3. Auswertung der Teilprüfungen durch die Prüfstelle.
4. Erstellung eines Endberichts durch die Prüfstelle, Übergabe an das BSI.
5. Zertifizierungsbescheinigung und Listung durch das BSI.

Als Nachweis der Zertifizierung erhält das Gerät ein vom BSI definiertes Qualitätssiegel, welches die Konformität des Gerätes zur TR-03119 dokumentiert.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
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.

Zwingend für Chipkartenleser sind zwei Hardwareschnittstellen und eine minimale Interface-Hardware.

Eine Schnittstelle dient zur Kommunikation mit dem Host. Über diese Schnittstelle wird der Chipkartenleser angesteuert. Mit dieser Kommunikationsschnittstelle muss es gleichzeitig möglich sein, Kommandos an den Chipkartenleser und an die Chipkarte zu senden. Selbstverständlich werden über diese Schnittstelle auch alle anderen Prozessdaten transportiert. Protokollumsetzer können hier auch in Softwaretreibern ausgeprägt sein.

Eine weitere Schnittstelle dient zur Kommunikation mit standardkonformem Chipkarten (ePA / Karte / Token). Hier werden, über eine Kontaktiereinheit oder kontaktlos, Daten zwischen Leser und Chipkarte ausgetauscht. Es ist wichtig, dass die elektrischen Eigenschaften und die Chipkartenprotokolle gemäß den zuständigen internationalen Normen ISO/IEC 7816 und ISO/IEC 14443 berücksichtigt werden und eine fehlerfreie Kommunikation gewährleisten. Bedienerschnittstellen in Form von Eingabe oder Ausgabegeräten sind optional möglich.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

	Cat-B	*Cat-S*	*Cat-K*	*Prüfvorschriften*
Umweltanforderungen	X	X	X	s. Anhang B.1
Funktionale Prüfung	X	X	X	s. Anhang B.2
kontaktlose Schnittstelle ISO/IEC 14443	X	X	X	TR-03105, Part 4 s. Anhang B.2
kontaktbehaftete Schnittstelle ISO/IEC 7816	O	O	X	Prüfung durch Prüfstelle
Pinpad (sichere PIN-Eingabe)	O	X	X	Sicherheitsbegutachtung durch Prüfstelle
PACE *	O	X	X	TR-03105, Part 5.2 (Profil PACE) s. Anhang B.2
ePA-QES	O	O	X	TR-03105, Part 5.2 (Profil QES) s. Anhang B.2 Bestätigung nach SigV
Display (2x16 alphanumerische Zeichen)	O	O	X	Sicherheitsbegutachtung durch Prüfstelle
Firmwareupdate	O	X	X	Sicherheitsbegutachtung durch Prüfstelle
Applikation im Leser	O	O	X	applikationsspezifische Prüfungen

* PACE wird beim Basis-Leser vollständig in der eCard-API abgebildet.

Tabelle 1: Übersicht Chipkartenleser-Kategorien

Im Folgenden werden drei Arten von Chipkartenlesern beschrieben:

- Einfachste Chipkartenleser sind oft generisch ausgeprägt, bzw. für eine bestimmte Anwendung konzipiert und unterstützen somit einige **Basis**funktionen, die aber durchaus von Applikationen mit ähnlichen Anforderungen genutzt werden können.
- Häufig findet man Chipkartenleser, die höheren qualitativen Ansprüche genügen, oft 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 sind als **Standard**-Leser zu bezeichnen und besitzen mindestens ein Pinpad zur sicheren PIN-Eingabe zur Freischaltung von Inhalten in kontaktlose und ggf. kontaktbehaftete Chipkarten.
- Eine weitere Kartenterminalvariante ist der **Komfort**-Leser, welcher aufgrund der Vielfältigkeit und **komfort**ablen Nutzungsvarianten eine Vielzahl von Anwendungen bedienen kann. Er besitzt mindestens ein Pinpad zur sicheren PIN-Eingabe zur Freischaltung von Inhalten in kontaktlose und kontaktbehaftete Chipkarten und ein Display mit 2x 16 alphanumerischen Zeichen, weiterhin befindet sich mindestens eine eigene Anwendung im Terminal.

Die vorliegende Technische Richtlinie betrachtet damit drei Chipkartenleserfamilien:

1. (**Cat-B**) - reine kontaktlose Basis-Chipkartenleser, die vornehmlich für den Gebrauch des ePAs und für technologieverwandte Anwendungsfälle gedacht sind.
2. (**Cat-S**) - multifunktionaler Standard-Chipkartenleser (bzw. Kartenterminal) mit kontaktloser Schnittstelle **und optional** mit kontaktbehafteter Schnittstelle. Das Gerät besitzt weiterhin mindestens ein Pinpad zur sicheren PIN-Eingabe.
3. (**Cat-K**) – multiapplikativer Komfort-Chipkartenleser (bzw. Kartenterminal) mit kontaktlosen **und** kontaktbehafteten Schnittstellen, mit mindestens einer eigenen Applikation, welche auch spezielle Anwendungen unterstützen, sowie einem Pinpad zur sicheren PIN-Eingabe zur Freischaltung von Inhalten in kontaktlose und kontaktbehaftete Chipkarten und ein Display mit 2x 16 alphanumerischen Zeichen.

Während der 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.

Des Weiteren ergeben sich durch die Anforderungen des Signaturgesetzes an die Signaturkomponente weitere Merkmale (siehe Anhang B.4).

In Tabelle 2 werden die drei Lesertypen den im Augenblick bekannten Medien und Anwendungen zugeordnet.

Der Anwender / Endnutzer erkennt die Ausprägungsvarianten aus der Produktdokumentation des Herstellers und aus den Zertifizierungsdokumenten.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Applikation / Leser		*Cat-B*	*Cat-S*	*Cat-K*
ePA	eID	X	X	X
	QES	-	O	X
VDV	Kernapplikation	X	X	X
ELENA-Verfahren	elektronischer Entgeltnachweis	-	O	X
ELSTER	elektronische Steuererklärung	O	O	X
eGK	Patientendaten	O	O	X
	eRezept	O	O	X
	QES	-	O	X
	Authentisierung	O	O	X
FinTS	HBCI	O	O	O
	TAN-Generierung	O	O	O
	(Q)ES	(-)O	O	O
	SECODER-Banking*	O	O	O
Elektronische Signatur mit Signaturkarten	QES	-	O	X
	fortgeschrittene elektronische Signatur (FES)	O	O	X

* Nach entsprechender Anpassung der SECODER-Spezifikation durch den ZKA bzw. einer entsprechenden Sicherheitsevaluierung, betr. zusätzlicher Hardwarekomponenten siehe ZKA Spezifikation SECODER Connected Mode Reader Applications 1.2, 21.12.2007, Kap. 2.7

Tabelle 2: Referenzanwendungen und zugeordnete Chipkartenleserkategorien

4 Basis-Chipkartenleser Cat-B

Zurzeit besteht bei den Bürgern keine geeignete Infrastruktur an Chipkartenlesern, die für die eGovernment-, und privatwirtschaftlichen Dienste des ePA genutzt werden könnte.

Die sukzessive Ausbreitung einer Infrastruktur an Chipkartenlesern ist eine Voraussetzung für den Ausbau des Angebots durch Dienstleister. Dienstanbieter benötigen dazu Informationen über die erwartete Marktdurchdringung, um die Reichweite der eigenen Angebote ermitteln zu können.

Die Implementierung einer Infrastruktur an Basis- Chipkartenlesern kann nur gelingen, wenn eine signifikante Anzahl von Bürgern auf Grund des zu erwartendem Nutzens bereit ist, die Technologie einzusetzen. Dies ist dann der Fall, wenn der Wert der Dienste, die mit dem Lesegerät genützt werden können, die Anschaffungskosten überwiegt.

Der Basis-Chipkartenleser soll dies in Form eines kostengünstigen Einsteigergeräts unterstützen.

4.1 Dienste

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

1. e-Government Dienste des ePA (z.B. Authentisierungsdienst, Rentenversicherung)

2. Altersverifikation
3. eTicketing nach VDV Kernapplikation (mit kontaktloser Karte entsprechend VDV Kernapplikation)
4. Wohnsitz- und Identitätsnachweis bei Internetshopping
5. Postident Ersatz

Das Lesegerät unterstützt bei diesen Anwendungen den Datenaustausch zwischen dem Trägermedium und dem jeweiligen Anwendungsserver im Internet. Dabei kommen je nach Anwendung neben dem ePA auch andere Trägermedien zum Einsatz. Auch gibt es bereits anwendungsspezifische Software für die jeweiligen Dienste. Tabelle 3 gibt eine exemplarische Übersicht.

Dienst	***Beschreibung***	***Kundenmedium***	***Anwendungssoftware / Middleware***
Authentisierungsdienst	Identitätsnachweis, Anlegen von Kundenkonten, Altersnachweis, etc	ePA	eCard-API / PC/SC
Elektronische Signatur	Nutzung einer elektronischen Signatur	Signaturkarte	eCard-API / PC/SC
VDV Kernapplikation	Nachladen von Berechtigungen	VDV Kundenmedium	eCard-API (nach Integration der VDV-KA)

Tabelle 3: Exemplarische Dienste und Trägermedien Cat-B

4.2 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. Beim ePA-Basisleser wird die Installation des Geräts 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 Diese müssen 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 Softwarepakete 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 dienstspezifische Software deinstalliert werden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

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.

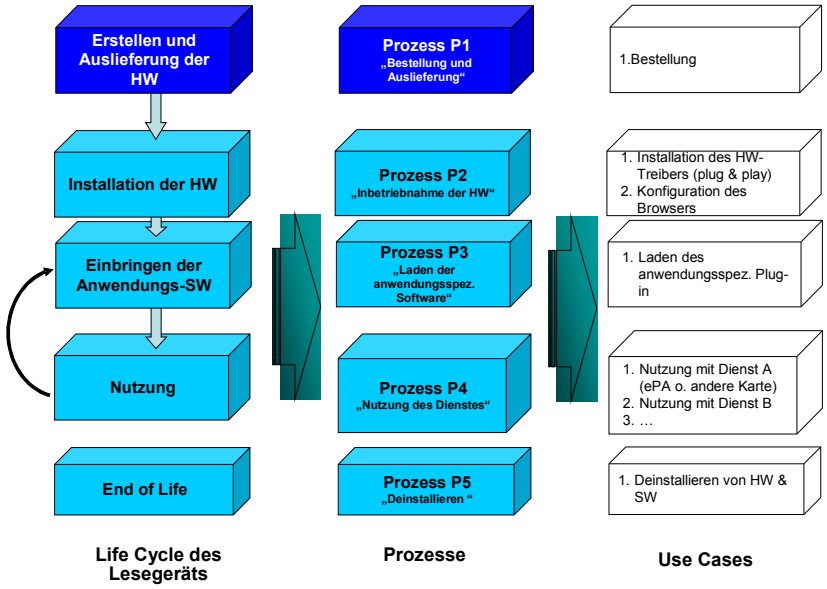

Abbildung 1 Life Cycle der generischen Lesegeräte

4.3 Heimanwendung

Für die Anwendung im Heimbereich zeigt Abbildung 2 das Gesamtsystem bei Nutzung des ePA-Basislesers.

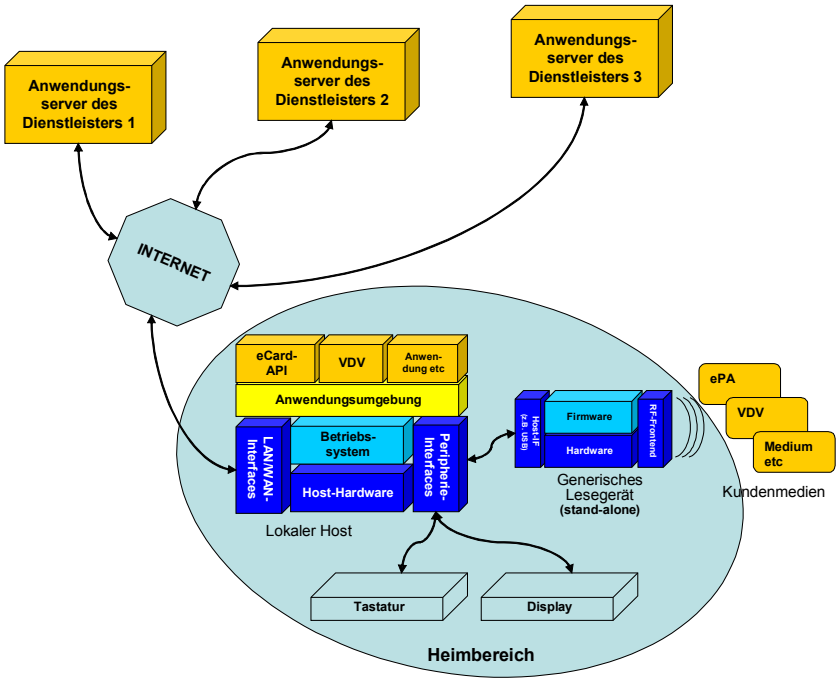

Abbildung 2: Gesamtsystem Cat-B

4.4 Grundlagenanforderungen und Annahmen

4.4.1 Optimierung des Verhältnisses von Kosten und Nutzen

1.1	Minimierung der Kosten des generischen Chipkartenlesers
Anforderung	Der Basis-Chipkartenleser soll preisgünstig sein.
Begründung	Zu Beginn des Aufbaus der Infrastruktur wird das Angebot an Diensten und somit der Nutzen für den Anwender noch begrenzt sein. Daher müssen die Anschaffungskosten in einer Größenordnung liegen, die aus Sicht des Bürgers ein „Ausprobieren“ zulässt oder alternativ für die Subventionierung geeignet ist.

1.1	**Minimierung der Kosten des generischen Chipkartenlesers**
Umsetzung	1. Einfache, anwendungsübergreifend zu nutzende Hardware. Beschränkung auf generische Unterstützung des ISO/IEC 14443-Protokolls. 2. Abbildung anwendungsspezifischer Funktionen durch lokale oder zentrale SW (z.B. eCard API) 3. Keine anwendungsspezifische Konfiguration der Hardware oder Firmware 4. Keine Spezialfunktionen in Hardware oder Firmware (Testfunktionen, etc) 5. Keine Tastatur, kein Display 6. Keine „Personalisierung“ des Chipkartenlesers 7. **Optional:** Investitionsschutz durch Updatefähigkeit

4.4.2 Anwenderfreundlichkeit

2.1	**Installation des ePA Basislesers**
Anforderung	Das Lesegerät muss auch durch Laien problemlos am PC zu installieren sein.
Begründung	Probleme oder signifikanter Aufwand bei der Installation der Anwendungssoftware führen zu Akzeptanzproblemen beim Anwender.
Umsetzung	1. Installation der Hardware mittels geeignetem Treiber an Standard-Schnittstelle des PC (z.B. USB) 2. Benutzerfreundliche Installation 3. Keine anwendungsspezifische Konfiguration der Hardware oder Firmware erforderlich. 4. Keine „Personalisierung“ des Chipkartenlesers.

2.2	**Anwenderservice**
Anforderung	Für den Fall von technischen Problemen muss dem Anwender eine einfache Möglichkeit zur Prüfung seines Chipkartenlesers mit ePA und – bei weiterführendem Support-Bedarf - ein technischer Kundenservice zur Verfügung stehen.
Begründung	Fehlfunktionen können bei dem Systemkonzept nicht nur durch das Lesegerät und den ePA sondern z.B. auch durch den PC oder weitere spezifische Anwendungssoftware verursacht werden. Eine Testfunktion, die automatisch ermittelt, ob generisches Lesegerät und der ePA funktionieren, hilft dem Kunden, Fehlerquellen auszuschließen und den richtigen Ansprechpartner für die Fehlerbehebung zu identifizieren. Für den Dienstanbieter reduziert eine solche Testfunktion das Aufkommen an Support-Anfragen. In jedem Fall ist jedoch ein Kundendienst für Lesegerät/ePA erforderlich. Anderenfalls ist mit Akzeptanzproblemen zu rechnen.
Umsetzung	1. Bereitstellung einer Testfunktion für das Lesegerät und den ePA im Internet. 2. Bereitstellung einer kostengünstigen Support-Hotline und FAQs auf der Website des Herstellers

2.3	**Unterstützung verschiedener Betriebssysteme**
Anforderung	Treiberunterstützung für die gängigen Betriebssysteme (siehe A.9)
Begründung	Für diese Betriebssysteme müssen Treiber und eine einheitliche API zur anwendungsspezifischen SW bereitgestellt werden, wenn eine hohe Marktdurchdringung erreicht werden soll.
Umsetzung	1. Bereitstellung von Treibern für alle relevanten Betriebssysteme. Integration der Treiber in eCard-API, andere anwendungsspezifische SW 2. Verwendung von Java-Plug-Ins für anwendungsspezifische Software 3. Nutzung einer eCard-API

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

4.5 Erforderliche Module

Für den Chipkartenleser Cat-B sind die in Tabelle 4 aufgezählten Eigenschaften obligatorisch.

Dem Interoperabilitätsgedanken folgend, sind daher die Module aus den Kapiteln des Anhangs A zu verwenden. Die aufgeführten Module sind gleichzeitig die Indikatoren für die Nachweise und Prüfungen (s. Kapitel 2.4) die für eine Zertifizierung gemäß dieser TR erforderlich sind.

Werden optionale Eigenschaften und Funktionen verwendet, so sind diese kompatibel zu den in den Kapiteln des Anhangs A beschriebenen Modulen auszuführen.

Die Konformität ist prüfungsrelevant und erfordert somit Zusatzprüfungen entsprechend den verwendeten Modulen.

Nr.	*Eigenschaft*	*Kapitel*	*Bemerkung*
1B-1	Fehlertoleranz	A.3	Fehlerbehebung bzw. Fehlerüberbrückung
1B-2	Elektrische Eigenschaften	A.1.1	Gemäß dem angepasstem ICAO Standard
1B-3	Hostinterface	A.1.5	Beschreibung und Nachweis
1B-4	Transport von Zeichen	A.2.1	Gemäß ISO/IEC 14443 Teil 2 und 3
1B-5	Chipkartenprotokolle	A.7.1	Nur kontaktlose Schnittstelle ISO/IEC 14443-4 (T=CL)
1B-6	Programmierschnittstelle	A.8	Nur PC/SC obligatorisch

Tabelle 4: Übersicht der Mindestanforderungen Cat-B

5 Standard-Chipkartenleser Cat-S

Chipkartenleser der Kategorie Cat-S unterstützen generische Chipkarten-Schnittstellenstandards für **kontaktlose** Chipkarten und können optional mit einer **kontaktbehafteten** Schnittstelle ausgestattet sein.

Der **Standard-Chipkartenleser ist zur sicheren PIN-Eingabe mindestens mit einem Pinpad sowie mit weiteren optionalen Komponenten** ausgestattet. Der Leser unterstützt das PACE Verfahren (siehe Anhang A.10.1).

Anwendungen wie die qualifizierte elektronische Signatur oder die Unterstützung von Bankenkarten sind optional.

5.1 Dienste

Der beschriebene Chipkartenleser kann für kontaktlose und **optionale** kontaktbehaftete Anwendungen und Dienste eingesetzt werden.

Tabelle 5 gibt eine **exemplarische** Übersicht über Dienste und damit verbundene Trägermedien.

Dienst	***Beschreibung***	***Trägermedium***	***Anwendungsoftware / Middleware***
Authentisierungsdienst	Identitätsnachweis, Anlegen von Kundenkonten, Altersnachweis, etc	ePA	eCard-API / PC/SC
Elektronische Signatur	Nutzung einer qualifizierten elektronischen Signatur	ePA, eGK, Anbieterspezifische Karte, Signatur Bankkarten	eCard-API / PC/SC
VDV Kernapplikation	Nachladen von Berechtigungen	VDV Kundenmedium	eCard-API (nach Integration der VDV-KA)
Patientendaten	Lesen privater Patientendaten im ungeschützten Bereich	eGK, KVK	eCard-API, CT-API
eRezept/ Onlineapotheken	Lesen von Rezeptdaten, Ordern von Medikamenten im Internet	eGK	eCard-API
HBCI/FinTS	Banktransaktionen im Internet	anbieterspezifische Karte	PC/SC
Geldkartenapplikation	Aufladen der Geldkarte	Geldkarte	PC/SC
Office Anwendungen	Remote Access, VPN, Passwort-Speicher, E-Mailverschlüsselung	anbieterspezifische Karte	PC/SC
eTicketing	Nachladen von Berechtigungen für Veranstaltungen (Sport, Konzerte, Events)	anbieterspezifische Karte	PC/SC

Tabelle 5: Exemplarische Dienste und Trägermedien Cat-S

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

5.2 Nutzungsprozesse und Use Cases

Alle Use Cases im Lebenszyklus des Chipkartenlesers müssen durch die Spezifikation der Chipkartenleser in Betracht gezogen werden. Folgende Besonderheiten sind dabei zu beachten:

1. Installation durch den Endanwender, besonders im Heimbereich
2. Im Laufe der Zeit können Updates der Firmware notwendig werden. Diese müssen vom Endanwender in einem sicheren Verfahren in den Leser eingebracht werden.
3. Beliebige der o.g. Dienste sollen das Gerät gleichzeitig nutzen können – soweit vom Gerät unterstützt und es die aufrufenden Software-Schichten erlauben (Stichwort: exklusiver Zugriff über PC/SC)
4. Deinstallation durch den Endanwender

5.3 Heimanwendung

In Abbildung 3 ist erkennbar, dass beim multifunktionalen Standardleser noch weitere Chipkarten und Anwendungen genutzt werden können.

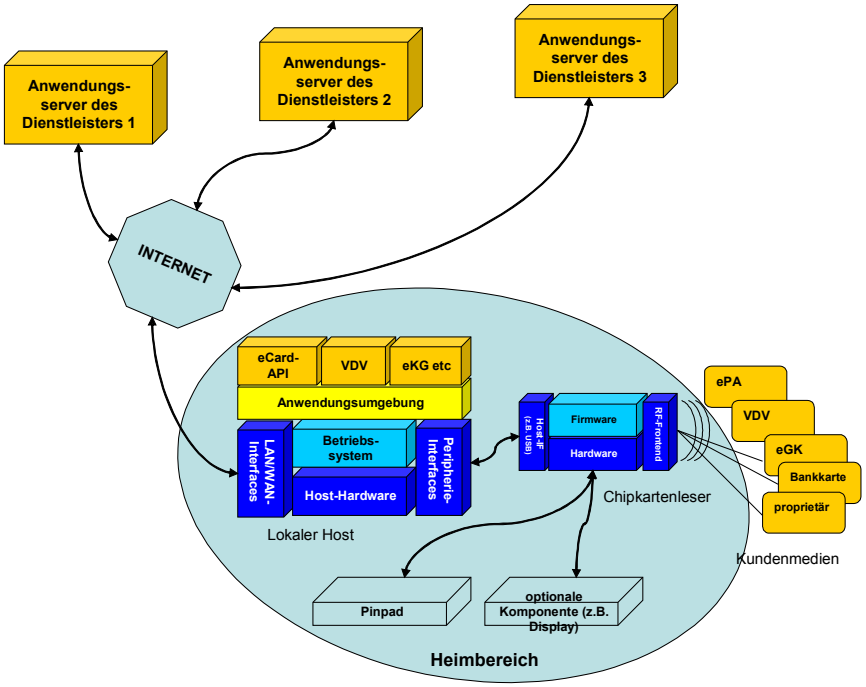

Abbildung 3: Gesamtsystem Cat-S

5.4 Grundlagenanforderungen und Annahmen

Folgende Eigenschaften sollen Chipkartenleser der Kategorie Cat-S aufweisen:

5.4.1 Sicherheit

1.1	**Sichere PIN-Eingabe**
Anforderung	Der Leser muss die sichere PIN-Eingabe unterstützen.
Begründung	Der Host-Rechner beim Endanwender ist ein potentielles Angriffsziel, wodurch die Geheimhaltung der PIN durch den Host nicht mehr gewährleistet werden kann. Um die PIN auch bei einem angegriffenen Host nicht preiszugeben, muss die sichere PIN-Eingabe benutzt werden.
Umsetzung	Sichere PIN-Eingabe mittels Pinpad und optionalen Komponenten (Anzeige des Kartenslots und Betriebszustand) am Kartenleser. Der Leser hat das PACE Verfahren implementiert.

1.2	**Sichere PIN-Übertragung über die kontaktlose Schnittstelle**
Anforderung	Der Leser darf nach der sicheren PIN-Eingabe die PIN nicht klarschriftlich über das kontaktlose Interface senden.
Begründung	Ein angegriffener Host könnte die sichere PIN-Eingabe einleiten, bevor Secure-Messaging aktiviert ist.
Umsetzung	Der Leser kontrolliert, ob Secure Messaging aktiviert ist, bevor die PIN über die kontaktlose Schnittstelle übertragen wird.

1.3	**Autarke Bildung des Schlüsselmaterials**
Anforderung	Das Schlüsselmaterial muss vollständig im Kartenleser gebildet werden.
Begründung	Der Kartenleser soll auch bei beidseitigen Angriffen, also angegriffenem Host und Ablauschen der Kartenkommunikation für die Geheimhaltung der PINs sorgen. Es ist es notwendig, dass nur der Kartenleser und die Karte das Schlüsselmaterial für das Secure Messaging kennen.
Umsetzung	Die Gewinnung des Schlüsselmaterials muss vollständig im Leser ablaufen. Hierfür hat der Leser das PACE Verfahren implementiert

5.4.2 Einsatzmöglichkeiten

2.1	Unterstützung verschiedener Betriebssysteme
Anforderung	Treiberunterstützung für die gängigen Betriebssysteme (siehe A.9)
Begründung	Für diese Betriebssysteme müssen Treiber und eine einheitliche API zur anwendungsspezifischen SW bereitgestellt werden, wenn eine hohe Marktdurchdringung erreicht werden soll.
Umsetzung	1. Bereitstellung von Treibern für alle relevanten Betriebssysteme. Integration der Treiber in eCard-API, andere anwendungsspezifische SW 2. Verwendung von Java-Plug-Ins für anwendungsspezifische Software 3. Nutzung einer eCard-API

5.4.3 Optimierung des Verhältnisses von Kosten und Nutzen

3.1	Optimierung der Kosten des Standard-Chipkartenlesers
Anforderung	Multifunktionaler Chipkartenleser
Begründung	Der Standard-Chipkartenleser soll dem Anwender die Möglichkeit bieten, mehrere Applikationen und Chipkarten mit einem Lesegerät zu nutzen.
Umsetzung	1. Heimbereich: Anwendungsübergreifend zu nutzende Hardware zur Schaffung eines Massenmarkts. 2. Keine anwendungsspezifischen Konfiguration der Hardware oder Firmware 3. Keine „Personalisierung“ des Chipkartenlesers

5.4.4 Anwenderfreundlichkeit

4.1	Installation des Standard Chipkartenlesers
Anforderung	Das Lesegerät muss auch durch Laien problemlos zu installieren sein.
Begründung	Probleme oder signifikanter Aufwand bei der Installation der Anwendungssoftware führen zu Akzeptanzproblemen beim Anwender. Kostenersparnis beim Support.
Umsetzung	1. Installation der Hardware mittels geeignetem Treiber an Standard-Schnittstelle des PC (z.B. USB) 2. Benutzerfreundliche Installation 3. Keine anwendungsspezifische Konfiguration der Hardware oder Firmware. 4. Keine Personalisierung des Chipkartenlesers 5. Bereitstellung einer kostengünstigen Support-Hotline und FAQs auf der Website des Herstellers

5.5 Erforderliche Module

Die Tabelle 6 enthält die Eigenschaften eines Cat-S Chipkartenlesers. Die Positionen 2S-1 bis 2S-15 sind obligatorisch, alle anderen Module sind optional und müssen nur bei Verwendung der Funktion/Hardwareausprägung beachtet werden.

Auch hier sind die aufgeführten Module die Indikatoren für die Nachweise und Prüfungen (s. Kapitel 2.4) die für eine Zertifizierung erforderlich sind.

Nr.	*Eigenschaft*	*Kapitel*	*Kategorie*	*Bemerkung*
2S-1	Fehlertoleranz	A.3	obligatorisch	Fehlerbehebung bzw. Fehlerüberbrückung
2S-2	Elektrische Eigenschaften kontaktlos / kontaktbehaftet	A.1.1	obligatorisch	Gemäß angepasstem ICAO, ISO/IEC 14443 bzw. ISO/IEC 7816 kontaktlos, optional: kontaktbehaftet
2S-3	Hostinterface	A.1.5	obligatorisch	Beschreibung und Nachweis
2S-4	Transport von Zeichen	A.2.1, A.2.3	obligatorisch	kontaktlos, optional: kontaktbehaftet
2S-5	Chipkartenprotokoll	A.7.1	obligatorisch	Nur ISO/IEC 14443 -4 (T=CL) obligatorisch
2S-6	Programmierschnittstelle	A.8	obligatorisch/ optional	Nur PC/SC obligatorisch
2S-7	Pinpad	A.14.4	obligatorisch	
2S-8	Sichere PIN-Eingabe	A.19	obligatorisch	Die PIN verlässt das Terminal nicht
2S-9	PACE Verfahren	A.10.1	obligatorisch	
2S-10	Firmwareupdate	A.16	obligatorisch	sicherer Download von Firmware-Updates
2S-11	Sicherheitsmodus Anzeige	A.14.2	obligatorisch	
2S-12	Umweltanforderungen	B.1	obligatorisch	Alle gesetzlichen Anforderungen
2S-13	Sicherheitsgutachten	B.3	obligatorisch	
2S-14	Verfügbarkeit	A.17	obligatorisch	Kein undefinierter Zustand
2S- 15	PACE Schlüsselerzeugung	A.12	obligatorisch	Benötigt für PACE-Verfahren
2S-16	ePA QES	B.4	optional	

2S-17	MTK-Modul	A.5	optional	MKT/CT-BCS gemäß der Hardwareausprägung
2S-18	Display	A.14.3	optional	
2S-19	Kontaktiereinheit	A.1.2	optional	50.000 Kontaktierungen
2S-20	ISO/EMV Umschaltung über mitgelieferte Tools des Herstellers	A.1.3	optional	Per HW oder SW
2S-21	Sicherheitsevaluierung und -bestätigung	B.3, B.4	optional	SigG, SigV

Tabelle 6: Übersicht der Anforderungen Cat-S

6 Komfort-Chipkartenleser Cat-K

Um neben dem ePA weitere Chipkarten wie VDV-Karte, Gesundheitskarte, Signaturkarte, Bankkarte und Geldkarte unterstützen zu können, sind für Büroanwendungen und für den Heimbereich komfortable und multifunktionale Kartenterminals mit Tastatur, Display und definierten Sicherheitsfunktionen erforderlich.

Die vorgebenden Anwendungen bestimmen die Ausprägung des Kartenterminals.

Vielfältige Funktionen bis hin zur qualifizierten elektronischen Signatur lassen ein breites Einsatzgebiet zu.

Kartenterminals des Typs Cat-K unterstützen das PACE-Verfahren (siehe Kapitel A.10) und besitzen eine sichere PIN-Eingabe für kontaktlose und kontaktbehaftete Chipkarten, ein Display mit 2 x 16 alphanumerischen Zeichen sowie mindestens eine eigene Applikation im Terminal (z.B. PACE). Chipkartenleser des Typs Cat-K können für kontaktlose und kontaktbehaftete Anwendungen und Dienste eingesetzt werden.

Im diesem Zusammenhang können nur Cat-S und Cat-K Leser die Geheimhaltung der PIN des ePAs garantieren. Weiterführend kann nur der Cat-K Leser die authentische Anzeige von Berechtigtem und Berechtigungen bei der eID-Funktion übernehmen.

6.1 Dienste

Tabelle 7 gibt eine **exemplarische** Übersicht über Dienste und damit verbundene Trägermedien.

Dienst	***Beschreibung***	***Trägermedium***	***Anwendungssoftware / Middleware***
Authentisierungsdienst	Identitätsnachweis, Anlegen von Kundenkonten, Altersnachweis, etc	ePA	eCard-API, PC/SC
Elektronische Signatur	Nutzung einer qualifizierten elektronischen Signatur	ePA optional: eGK, Anbieterspezifische Karte, Signatur Bankkarten	eCard-API, PC/SC
VDV Kernapplikation	Nachladen von Berechtigungen	VDV Kundenmedium	eCard-API (nach Integration der VDV-KA) PC/SC
Patientendaten	Lesen privater Patientendaten im ungeschützten Bereich	eGK, KVK	eCard-API, CT-API, PC/SC
eRezept/ Onlineapotheken	Lesen von Rezeptdaten, Ordern von Medikamenten im Internet	eGK	eCard-API, PC/SC
HBCI/FinTS	Banktransaktionen im Internet	Bankenkarte	Bankingsoftware, PC/SC
Geldkartenapplikation	Aufladen der Geldkarte	Geldkarte	Webapplikation, PC/SC

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Dienst	*Beschreibung*	*Trägermedium*	*Anwendungssoftware / Middleware*
Office Anwendungen	Remote Access, VPN, Passwort-Speicher, E-Mailverschlüsselung	anbieterspezifische Karte	CSP / PKCS#11, PC/SC
eTicketing	Nachladen von Berechtigungen für Veranstaltungen (Sport, Konzerte, Events)	anbieterspezifische Karte	Webapplikation, PC/SC

Tabelle 7: Exemplarische Dienste und Trägermedien Cat-K

6.2 Nutzungsprozesse und Use Cases

Alle Use Cases im Lebenszyklus des Chipkartenlesers müssen durch die Spezifikation der Chipkartenleser in Betracht gezogen werden. Folgende Besonderheiten sind dabei zu beachten:

1. Installation durch den Endanwender, besonders im Heimbereich
2. Im Laufe der Zeit können Updates der Firmware notwendig werden. Diese müssen vom Endanwender in einem sicheren Verfahren in den Leser eingebracht werden.
3. Beliebige der o.g. Dienste sollen das Gerät gleichzeitig nutzen können – soweit vom Gerät unterstützt und es die aufrufenden Software-Schichten erlauben (Stichwort: exklusiver Zugriff über PC/SC)
4. Deinstallation durch den Endanwender

6.3 Heimanwendung

In Abbildung 4 ist erkennbar, dass beim multifunktionalen Komfortleser im Vergleich zum Basisleser weitere Chipkarten und Anwendungen genutzt werden können.

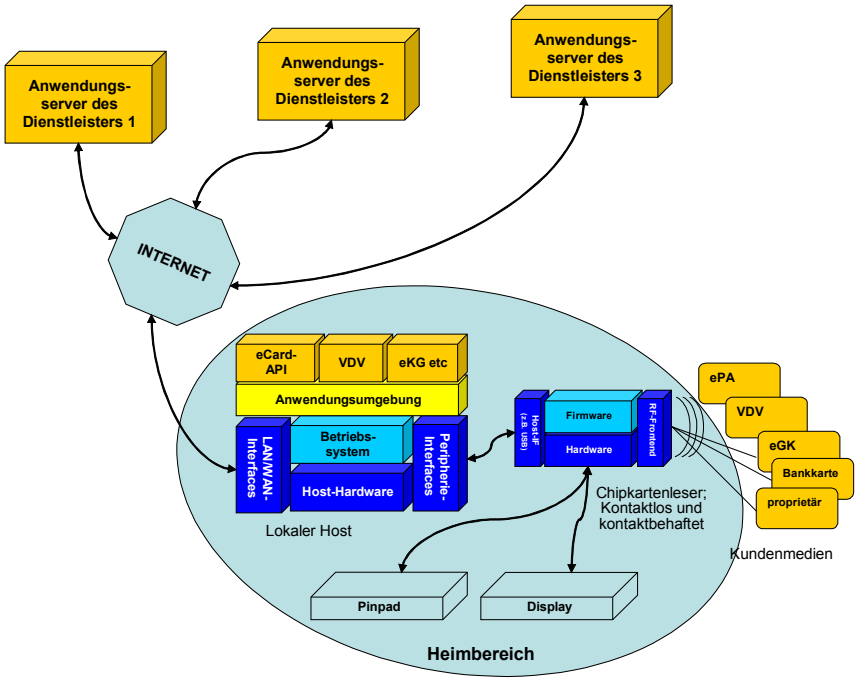

Abbildung 4: Gesamtsystem Cat-K

6.4 Grundlagenanforderungen und Annahmen

Folgende Eigenschaften sollen Chipkartenleser der Kategorie Cat-K aufweisen:

6.4.1 Sicherheit

1.1	**Sichere PIN-Eingabe**
Anforderung	Der Leser muss die sichere PIN-Eingabe unterstützen.
Begründung	Der Host-Rechner kann beim Endanwender angegriffen sein, wodurch die Geheimhaltung der PIN durch den Host nicht mehr gewährleistet ist. Um die PIN auch bei einem angegriffenem Host nicht preiszugeben, muss die sichere PIN-Eingabe benutzt werden
Umsetzung	Sichere PIN-Eingabe mittels Pinpad und optionalen Komponenten (Anzeige des Kartenslots und Betriebszustand) am Kartenleser.

1.2	**Sichere PIN-Übertragung über die kontatklose Schnittstelle**
Anforderung	Der Leser darf nach der sicheren PIN-Eingabe die PIN nicht klarschriftlich über das kontaktlose Interface senden.
Begründung	Ein angegriffener Host könnte die sichere PIN-Eingabe einleiten, bevor Secure-Messaging aktiviert ist.
Umsetzung	Der Leser kontrolliert, ob Secure Messaging aktiviert ist, bevor die PIN über die kontaktlose Schnittstelle übertragen wird.

1.3	**Autarke Bildung des Schlüsselmaterials**
Anforderung	Das Schlüsselmaterial muss vollständig im Kartenleser gebildet werden
Begründung	Der Kartenleser soll auch bei beidseitigen Angriffen, also angegriffenem Host und Ablauschen der Kartenkommunikation für die Geheimhaltung der PINs sorgen. Es ist es notwendig, dass nur der Kartenleser und die Karte das Schlüsselmaterial für das Secure Messaging kennen.
Umsetzung	Die Gewinnung des Schlüsselmaterials muss vollständig im Leser ablaufen. Hierfür hat der Leser das PACE Verfahren implementiert

1.4	**Authentische Anzeige des Berechtigten und der Berechtigungen**
Anforderung	Der Zugriffsberechtigte und dessen Berechtigungen sollen am Display des Lesers angezeigt werden.
Begründung	Ein angegriffener Host kann die Authentizität dieser Anzeigen nicht mehr gewährleisten.
Umsetzung	Der Leser zeigt bevor der Anwender die PIN zum Aufbau des PACE – Tunnels eingibt, den Berechtigten und dessen Berechtigungen an und überwacht nach Aufbau des PACE - Tunnels die Übertragung des Berechtigungszertifikats auf Übereinstimmung mit den zuvor angezeigten Daten.

6.4.2 Einsatzmöglichkeiten

2.1	**Unterstützung verschiedener Betriebssysteme**
Anforderung	Treiberunterstützung für die gängigen Betriebssysteme (siehe A.9)
Begründung	Für diese Betriebssysteme müssen Treiber und eine einheitliche API zur anwendungsspezifischen SW bereitgestellt werden, wenn eine hohe Marktdurchdringung erreicht werden soll.
Umsetzung	1. Bereitstellung von Treibern für alle relevanten Betriebssysteme. Integration der Treiber in eCard-API, andere anwendungsspezifische SW 2. Verwendung von Plug-Ins für anwendungsspezifische Software 3. Nutzung der eCard-API

6.4.3 Optimierung des Verhältnisses von Kosten und Nutzen

3.1	**Optimierung der Kosten des Komfort-Chipkartenlesers**
Anforderung	Multifunktionaler Chipkartenleser
Begründung	Der Komfort-Chipkartenleser soll dem Anwender die Möglichkeit bieten, mehrere Applikationen und Chipkarten mit einem Lesegerät zu nutzen.
Umsetzung	1. Heimbereich: Anwendungsübergreifend zu nutzende Hardware zur Schaffung eines Massenmarkts. 2. Keine anwendungsspezifischen Konfiguration der Hardware oder Firmware 3. Keine „Personalisierung“ des Chipkartenlesers

6.4.4 Anwenderfreundlichkeit

4.1	**Installation des Komfort-Chipkartenlesers**
Anforderung	Das Lesegerät muss auch durch Laien problemlos zu installieren sein.
Begründung	Probleme oder signifikanter Aufwand bei der Installation der Anwendungssoftware führen zu Akzeptanzproblemen beim Anwender. Kostenersparnis beim Support.
Umsetzung	1. Installation der Hardware mittels geeignetem Treiber an Standard-Schnittstelle des PC (i.d.R.. USB) 2. Benutzerfreundliche Installation 3. Keine Personalisierung des Chipkartenlesers 4. Bereitstellung einer kostengünstigen Support-Hotline

6.5 Erforderliche Module

Die Tabelle 8 enthält die Eigenschaften eines Cat-K Chipkartenlesers.

Auch hier sind die aufgeführten Module die Indikatoren für die Nachweise und Prüfungen (s. Kapitel 2.4) die für eine Zertifizierung erforderlich sind.

Nr.	***Eigenschaft***	***Kapitel***	***Kategorie***	***Bemerkung***
3K-1	Fehlertoleranz	A.3	obligatorisch	Fehlerbehebung bzw. Fehlerüberbrückung
3K-2	Elektrische Eigenschaften kontaktlos / kontaktbehaftet	A.1.1	obligatorisch	Gemäß dem angepasstem ICAO / ISO
3K-3	Hostinterface	A.1.5	obligatorisch	Beschreibung und Nachweis
3K-4	Transport von Zeichen	A.2.1, A.2.3	obligatorisch	kontaktlos, kontaktbehaftet

3K-5	Chipkartenprotokoll	A.7.1	obligatorisch	
3K-6	Programmierschnittstelle	A.8	obligatorisch/ optional	Nur PC/SC obligatorisch
3K-7	Pinpad	A.14.4	obligatorisch	
3K-8	Display	A.14.3	obligatorisch	
3K-9	Sichere PIN-Eingabe	A.19	obligatorisch	Die PIN verlässt das Terminal nicht
3K-10	PACE Verfahren	A.10.1	obligatorisch	
3K-11	Firmwareupdate	A.16	obligatorisch	sicherer Download von Firmware-Updates
3K-12	Sicherheitsmodus Anzeige	A.14.2	obligatorisch	
3K-13	Kontaktiereinheit	A.1.2	obligatorisch	50.000 Kontaktierungen
3K-14	Umweltanforderungen	B.1	obligatorisch	Alle gesetzlichen Anforderungen
3K-15	Sicherheitsgutachten	B.3	obligatorisch	
3K-16	Verfügbarkeit	A.17	obligatorisch	Kein undefinierter Zustand
3K-17	Applikation im Kartenterminal		obligatorisch	
3K-18	PACE Schlüsselerzeugung	A.12	obligatorisch	Benötigt für PACE-Verfahren
3K-19	ePA QES	B.4	obligatorisch	
3K-20	Sicherheitsevaluierung und -bestätigung	B.3,B.4	obligatorisch	SigG, SigV
3K-21	MTK-Modul	A.5	optional	MKT/CT-BCS gemäß der Hardwareausprägung
3K-22	ISO/EMV Umschaltung über mitgelieferte Tools des Herstellers	A.1.3	optional	Per HW oder SW

Tabelle 8: Übersicht der Anforderungen Cat-K

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.

Falls jedoch die Ausprägung oder die Funktionseinheit vorhanden ist, so sind ausschließlich die anschließend definierten Modulbeschreibungen zu berücksichtigen.

Werden zum Beispiel zur Karte Übertragungsprotokolle verwendet, die hier in einem Modul beschrieben sind, so sind diese entsprechend dieser TR (normgerecht) zu implementieren.

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

Die Profile ab Kapitel 3 beschreiben die Verwendung der einzelnen Module für den jeweiligen Chipkartenlesertyp.

A.1 Elektrische Eigenschaften

Generell werden bei allen Lesertypen dieser Spezifikation primär **kontaktlose Chipkarten** unterstützt.

A.1.1 Kontaktlose Schnittstelle

Kontaktlose Chipkartenleser erfüllen die Anforderungen gemäß der Normenreihe ISO/IEC 14443 – proximity cards (Teil 2 bis Teil 4) [PICC2-4] einschließlich des spezifizierten Feldstärkenbereichs.

Die Prüfungen orientieren sich an der korrespondierenden Norm ISO/IEC 10373-6.

Alle ePA Chipkartenleser erfüllen die informativen Forderungen für „Class1-PICC“ Lesegeräte.

Die elektrischen Eigenschaften sind so zu wählen, dass sie den Anforderungen für Chipkarten gemäß der Norm ISO/IEC 14443-2 [PICC2] entsprechen und Chipkarten vom Typ A und vom Typ B bei einer Frequenz von 13,56 MHz unterstützen.

Als Zertifizierungsreferenz ist die BSI TR-03105 [TR-03105] „Conformity Tests for Official Electronic ID Documents“ in der aktuellen und veröffentlichten Fassung zu verwenden.

A.1.2 Kontaktbehaftete Schnittstelle

Multifunktionale Lesertypen können alternativ auch **kontaktbehaftete Chipkarten** unterstützen.

In dem Fall müssen die Anforderungen der ISO/IEC 7816-3 [ISO3] (für Chipkarten) beachtet werden dass der Chipkartenleser Chipkarten, deren elektrische Eigenschaften sich konform zum Standard ISO/IEC 7816-3 [ISO3] verhalten, unter den dort genannten Bedingungen ohne Ausfälle bedienen können muss und eine Beschädigung der Chipkarten sicher ausgeschlossen wird.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Zusätzlich zu den Anforderungen in ISO/IEC 7816-3 [ISO3] muss der Chipkartenleser durch geeignete Maßnahmen gewährleisten, dass vor der Aktivierung und nach der Deaktivierung der Chipkarte die Spannungen an den Kontakten V_{cc}, I/O, CLK und RST gegenüber GND unter allen Umständen auch bei starken Einflüssen in dem von der ISO/IEC 7816-3 [ISO3] geforderten Bereich bleiben, so dass ein Schutz der Chipkarte gegen Fehlverhalten oder Beschädigung im nicht aktiven Zustand gewährleistet ist.

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

Der Chipkartenleser beliefert die Chipkarte standardmäßig mit einer Versorgungsspannung von 5 V, der Class A nach ISO/IEC 7816-3 [ISO3].

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 der ISO/IEC 7816-3.

A.1.3 ISO/EMV Umschaltung

Optional können Applikationen des Kreditwesens unterstützt werden. Maßgeblich sind hierzu die Anforderungen des EMV2000 [EMV2000] Standards. Da nicht beide Standards identisch sind, ist eine Umschaltmöglichkeit im Chipkartenleser vorzusehen, falls beide Standards unterstützt werden.

Hierzu ist insbesondere auch ein Chipkartenleserkommando zur Umschaltung gemäß Kapitel A.6 zu verwenden.

A.1.4 Erweiterung der elektrischen Eigenschaften

Es ist dafür zu sorgen, dass die Kontakte einer Kontaktiereinheit bei kontaktbehafteten Chipkarten, auch bei Einwirkung durch äußere Einflüsse, nicht den vorgeschriebenen Bereich der zuständigen Norm ISO/IEC 7816-3 [ISO3] verlassen. Dieses gilt gleichermaßen für den aktiven Betrieb während der Anwendung, als auch im inaktiven Zustand beim Einschieben der Chipkarte.

Chipkartenleser außerhalb üblicher Büroanwendungen (Systemleser) sind häufiger störenden elektrischen Einflüssen ausgesetzt. Es müssen zu den Anforderungen aus dem Kapitel A.1 zusätzliche Auflagen erfüllt werden, die in einer späteren Version dieser Technischen Richtlinie spezifiziert werden

A.1.5 Qualifizierung des Interfaces zum Host-System

Ein Hardware-Interface (z.B. USB 2.0, RS-232, Bluetooth®) zwischen Kartenleser und Hostsystem muss in seiner Ausprägung technisch beschrieben werden und wenn technisch möglich, geprüft und qualifiziert werden.

A.2 Transport von Zeichen

A.2.1 Kontaktlose Karte

Ein Chipkartenleser unterstützt die Protokolltypen TYP A und TYP B nach ISO/IEC 14443.

Der Betrieb von kontaktlosen Chipkarten durch den Chipkartenleser erfolgt gemäß der Norm 14443-2 [PICC2], 14443-3 [PICC3] und 14443-4 [PICC4]. Gemäß dem folgenden Ablauf muss der Chipkartenleser entsprechende Funktionen unterstützen:

- Aktivierung der Chipkarte (Request, Antikollisionsschleife und Select)
- Auslesen der UID
- ATS („Answer To Select“) / ATQB (“Answer To reQuest, Type B” wird gelesen
- ATS / ATQB Auswertung
- Protokoll-Parameter-Auswahl PPS („protocol and parameter selection“)
- Informationsaustausch mit der Chipkarte
- Deselektierung der Chipkarte

Der Chipkartenleser unterstützt PPS und höherer Taktfrequenzen in Übereinstimmung mit ISO/IEC 14443-4 [PICC4].

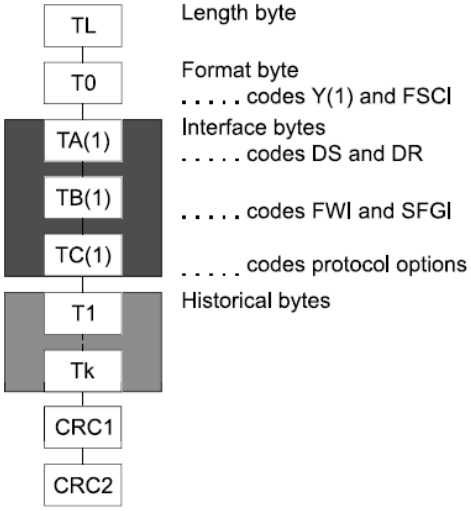

Abbildung 5: Aufbau des ATS gemäß ISO/IEC 14443-4

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

A.2.2 ATS/ATR kontaktloser Karten

Bei der Umstellung von kontaktbehafteten Karten auf kontaktlose Karten kann es erforderlich sein, bei einem Reset einen ISO/IEC 7816-3 [ISO3] konformen ATR an die Applikation zu melden.

Dieses ist insbesondere bei Verwendung der Chipkartenleserkommandos RESET, RESET CT und REQUEST ICC zweckmäßig.

Hierzu sollen einheitlich aus dem ATS gemäß ISO/IEC 14443-4 [PICC4], s.a. Abbildung 5, die „historical bytes“ isoliert und in nachfolgend beschriebenes ATR konvertiert werden (siehe auch ISO/IEC 7816-4 [ISO4]).

Zahlenwerte in hexadezimaler Notation:

TS	*T0*	*TD1*	*TD2*	*T1..T.k historical bytes*	*TCK*
3B	8k *	80	01	bb cc ...	XOR

* k= Anzahl der historical bytes (0-F)

Beispiel:

3B 87 80 01 4A 41 2D 30 37 90 00 B7

A.2.3 Kontaktbehaftete Karte

Der Betrieb von asynchronen, kontaktbehafteten Chipkarten durch den Chipkartenleser erfolgt konform zu ISO/IEC 7816-3. 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/IEC 7816-3 zur Erzielung höherer Datenübertragungsraten unbedingt 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/IEC 7816-3 aus. Bei fehlendem oder inkorrekt empfangenem ATR einer asynchronen Chipkarte kann die Aktivierung vom Chipkartenleser noch maximal zweimal wiederholt werden. Bei nicht erfolgreicher Aktivierung der Chipkarte wird diese vom Chipkartenleser deaktiviert.

Erhält der Chipkartenleser keinen ATR entsprechend ISO/IEC 7816-3 [ISO3] 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/IEC 7816-10 [ISO10] 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/IEC 7816-3 deaktiviert.

Unterstützt der Chipkartenleser eine manuelle Protokollauswahl, so bleiben bei nicht erfolgreicher Aktivierung der Chipkarte die Kontakte des Chipkartenlesers bis zu einer expliziten Deaktivierung aktiviert, um die Auswahl des Übertragungsprotokolls durch den Anwender zu ermöglichen.

A.3 Fehlertoleranz

Der Chipkartenleser muss bei jeder Inbetriebnahme, nach einem Reset und im laufenden Betrieb Fehlerzustände erkennen. Dabei sind Fehler der Hardware, Übertragungsfehler, Bedienungsfehler (ungültige Eingaben) und Fehler der Chipkarte zu signalisieren.

Tritt ein Fehler auf, so muss der Chipkartenleser durch interne Abläufe versuchen, den aufgetretenen Fehler automatisch zu beheben (z. B. Re-Synchronisation der Chipkarte / Chipkartenleser) oder zu überbrücken. Nach einer automatischen Fehlerbehebung bzw. Fehlerüberbrückung muss der Chipkartenleser kontinuierlichen Betrieb gewährleisten können. Ist eine automatische Fehlerbehebung bzw. -überbrückung des Chipkartenlesers nicht möglich, signalisiert der Chipkartenleser einen Fehler/Alarm und kann erst nach einem Reset weiter betrieben werden

A.4 Physikalische Kartendimensionen und Kontaktiereinheit

Der ePA in der Bauform TD-1 (85,6 mm x 54,0 mm x 1,25mm) muss vom Kartenleser unterstützt werden. Der Kartenleserhersteller hat im Rahmen der Prüfung sicherzustellen, dass durch die Verwendung des Kartenlesers keine Gefahr für die physische Unversehrtheit des ePA ausgeht.

Ein multifunktionaler Chipkartenleser, welcher kontaktbehaftete Chipkarten unterstützt, besitzt mindestens eine Kontaktiereinheit zur Aufnahme von Chipkarten der Größe ID-1 (85,6 mm x 54,0 mm x 0,80 mm) entsprechend der Norm ISO/IEC 7810 [ISO1].

Die Lage und die Zuordnung der Kontakte ergibt sich aus ISO/IEC 7816-2 [ISO2].

Darüber hinaus kann der Chipkartenleser optional weitere Kontaktiereinheiten besitzen. Diese können auch für das Format ID-000 (Plug-in-Karte) nach CEN ENV 1375-1 [CEN1375] ausgelegt sein.

A.5 MKT Modul

Im deutschen Finanz- und Gesundheitswesen, sowie bei Chipkartenleser für Signaturanwendungen, bis hin zu Anwendungen von Konzernausweisen bei Firmen, hat sich ein Kommandosatz nach dem Muster des internationalen Standards ISO/IEC 7816-4 [ISO4] etabliert.

Dieser wird in der MKT Spezifikation [MKT] Teil 4 definierte Basic Command Set (BCS) sowie ergänzend für synchrone Chipkarten der Teil 7 der MKT Spezifikation detailliert beschrieben.

Spezielle Kommandos zur Anwendung von synchronen Chipkarten sind in Kapitel A.13 aufgeführt.

Zusätzliche Chipkartenleserkommandos sind zugelassen, wenn sie funktionelle und sicherheitstechnische Eigenschaften nicht negativ beeinflussen.

A.6 Kommando zur EMV/ISO Umschaltung

Über den SET Interface Parameter Befehl kann die Möglichkeit geschaffen werden, von einer Anwendung das Verhalten des Lesers umzuschalten. Die technischen Details hierzu werden in einer späteren Version der TR-03119 fortgeschrieben.

A.7 Chipkartenprotokolle

Ein multifunktionaler Chipkartenleser unterstützt nachfolgend aufgeführte synchrone und asynchrone Übertragungsprotokolle zu den entsprechenden Chipkarten. Die Protokolle sind komplett nach den Vorgaben der jeweiligen internationalen Normen zu implementieren. Dazu gehören neben der Unterstützung der fehlerfreien Kommunikation in allen Variationsmöglichkeiten, wie z. B. Feldgrößenänderung, Wartezeitverlängerung, Datenverkettung, Resynchronisation und Kommunikationsabbruch auch die vollständige Erkennung und Korrektur von Übertragungsfehlern. Insbesondere muss allen Fehlerfällen wirksam begegnet werden und es darf keine Deadlock-Situation auftreten.

Die Unterstützung weiterer Chipkartenprotokolle wird durch diese TR nicht ausgeschlossen, diese müssen im ATR/ATS angezeigt werden.

Bei dedizierten Anwendungen kann die Unterstützung der notwendigen Chipkartenprotokolle begrenzt werden.

A.7.1 Kontaktloses Chipkartenprotokoll

- T=CL, Block orientiertes Halbduplex-Protokoll nach ISO/IEC 14443-4 [PICC4]

A.7.2 Asynchrone Chipkartenprotokolle

- T=1, Block orientiertes Halbduplex-Protokoll nach ISO/IEC 7816-3 [ISO3]
- T=0, Zeichen orientiertes Halbduplex-Protokoll nach ISO/IEC 7816-3 [ISO3]

1.1.1 Synchrone Chipkartenprotokolle

- S=10 für 2-Wire-Bus Chipkarten nach Herstellerspezifikation und ISO/IEC 7816-10 [ISO10]
- S=8 für I2C-Bus Chipkarten nach Herstellerspezifikation und ISO/IEC 7816-10 [ISO10]
- S=9 für 3-Wire-Bus Chipkarten nach Herstellerspezifikation und ISO/IEC 7816-10 [ISO10]

Weitere Informationen zur Nutzung von synchronen Chipkarten sind in Kapitel A.13 zu finden.

A.8 CT-API und PC/SC

Werden keine High-Level APIs zur Verfügung gestellt, so können andere APIs genutzt werden.

Kompatibel zu Anwendungen des Gesundheitswesens können CT-API Treiber genutzt werden.

Bei betriebsystemnahen Implementierungen (insbesondere bei MS Windows®) können PC/SC Schnittstellen genutzt werden.

Die CT-API [CT-API] ist prinzipiell ein reiner Schnittstellentreiber bei dem betriebsystemunabhängig und unabhängig von der physikalischen Schnittstelle Kommandos von der Anwendung abgesetzt werden können.

PC/SC [PC/SC] ist ein von der PC/SC-Workgroup entwickelter Standard für den Zugriff von PC-Anwendungen auf ein Smartcard-Lesegerät. Seit der Version 2.0 unterstützt dieser Standard auch andere Betriebssysteme. Ein Update der Schnittstellentreiber auf zukünftige und weitere Versionen der Betriebssysteme muss möglich sein und vom Lieferanten auf Anforderung bereitgestellt werden.

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.9 Unterstützte Betriebssysteme für PC-Systeme

Da der Bürgerclient unter den unten aufgeführten Betriebssystemen lauffähig ist, müssen die Kartenleser diese Betriebssysteme ebenso unterstützen:

- Windows® 2000
- Windows® XP
- Windows® Vista
- Windows® 7
- Mac™OS 10.5 und höher
- Debian 5.0 (Kernel Version 2.6.26) und höher
- Ubuntu 9.04 (Kernel Version 2.6.29) und höher
- OpenSuse 11.1 (Kernel Version 2.6.27) und höher

A.10 PACE

Die im Folgenden beschriebenen Funktionen werden wie in Kapitel A.11 beschrieben auf die in PC/SC verfügbare Funktion ScardControl abgebildet.

Das PACE-Verfahren dient dem Aufbau einer sicheren End-to-End Verbindung zwischen einem berechtigten eBusiness- oder eGovernment-Dienstleister und dem Chip des elektronischen Personalausweises. Die hierfür verwendeten Sicherheitsmechanismen basieren auf den Protokollen der Extended Access Control (EAC) des ePass. Die bereits existenten Protokolle Terminal-Authentisierung und Chip-Authentisierung wurden dabei um das PACE-Verfahren zur Absicherung der Luftschnittstelle zwischen Terminal und ePA erweitert.

Bei Verwendung eines Standard- oder Komfortlesers wird PACE direkt im Kartenterminal ausgeführt. Bei Verwendung von Basislesern wird PACE durch den User PC ausgeführt. Abbildung 6 zeigt den Aufbau der EAC-Verbindung mit PACE.

Mittels der Funktion GetReadersPACECapabilities() wird festgestellt, ob der Leser PACE unterstützt, es sich also um einen Cat-B, Cat-S oder Cat-K Leser handelt.

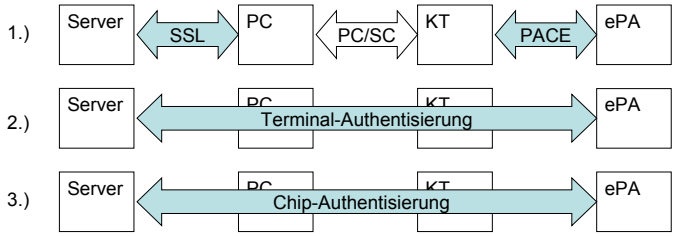

Abbildung 6: Aufbau EAC-Verbindung mittels PACE

A.10.1 Aufbau PACE-Tunnel mit Cat-S und Cat-K Lesern

Ist ein Standard- oder Komfortleser angeschlossen und es wird der entsprechende Rückgabewert geliefert, wird das PACE-Verfahren durchgeführt. Zur Durchführung des PACE Verfahren werden die CAT-S und CAT-K Leser um die Funktion EstablishPACEChannel(InputData) erweitert:

A.10.1.1 EstablishPACEChannel (InputData)

Die Funktion EstablishPACEChannel(InputData) dient zum Aufbau des PACE-Kanals sowie zum Abrufen von eID-Informationen vom ePA. Im Folgenden wird der Ablauf des PACE Verfahren zum Aufbau des PACE-Kanals mit der Funktion EstablishPACEChannel(InputData) beschrieben. Abbildung 7 gibt einen Überblick über die einzelnen Schritte.

Chip	*Kartenleser*	*Host-Rechner*
	EstablishPACEChannel(InputData)	
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		
	Eingabe der PIN Berechnung Kπ	
General Authenticate Step 3+4 Berechnung des Schlüsselmaterials für SM		

Abbildung 7: Ablauf PACE

- Der Kartenleser liest das EF_CardAccess und extrahiert die für das PACE - Verfahren notwendigen Parameter

- Der Kartenleser extrahiert aus InputData die PIN – ID (PIN, CAN, MRZ, PUK) und sucht nach dem optional in den InputData enthaltenem CHAT um die Rolle des Terminals zu kontrollieren. Entsprechend der Rolle des Terminals (Authentisierungsterminal, Signaturterminal) wird das das PACE – Protokoll eingeleitet:
  - MSE: Set AT
  - General Authenticate Step 1+2
- Der Kartenleser fordert (sofern nicht in den InputData enthalten) zur PIN Eingabe auf und leitet danach Kπ ab. Gegebenenfalls kann der Kartenleser parallel zur PIN - Eingabe bereits General Authenticate Step 2 und die Mappingfunktion durchführen.
- Der Kartenleser entschlüsselt das ‚Encrypted Nonce' mit Kπ
- Der Kartenleser bereinigt den Speicher von Informationen die Rückschlüsse auf die PIN zulassen
- Der Kartenleser führt die restlichen Schritte General Authenticate Step 3+4 durch und bildet das Schlüsselmaterial für das SM

In der Rolle eines Signaturterminals führen zugelassene Terminals im Anschluss an den Aufbau des PACE-Kanals direkt Terminal Authentication und Chip Authentication durch und bauen den neuen Tunnel auf.

A.10.1.2 Fehlerantworten

Im Fehlerfall werden die folgenden Fehlerantworten zurückgegeben:

Die Karte unterstützt das PACE – Verfahren nicht
Der Kartenleser unterstützt den ermittelten Algorithmus nicht
Input enthält unerwartete Daten
Negative Antwort der Karte auf General Authenticate Step 1-4
Kommunikationsabbruch mit Karte
Keine Karte im Feld
Abbruch durch Benutzer
Time-out durch Benutzer

A.10.2 Abfrage von eID-Informationen vom ePA durch Leser mit Display

Der Kartenleser muss die authentische Anzeige von Berechtigtem und Berechtigungen gewährleisten. Zur Realisierung werden die InputData der Funktion EstablishPaceChannel optional um die Zertifikatsbeschreibung erweitert.

Der Ablauf des PACE Verfahren zur Abfrage von eID-Informationen vom ePA gestaltet sich mit EstablishPACEChannel (InputData) wie folgt:

Chip	*Kartenleser*	*Host-Rechner*
	EstablishPACEChannel(InputData)	
Extrahieren der für PACE notwendigen Parameter aus EF_CardAccess		
	PIN-ID aus InputData Prüfung auf Rolle Authentisierungsterminal	
MSE: Set AT General Authenticate Step 1+2		
	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 SM		
	Bei ‚PSO: Verify Certificate' Vergleich HASH aus Certficate Extensions mit Variable StoreHASH	

Abbildung 8: Ablauf PACE mit Display

A.10.2.1 EstablishPACEChannel(InputData)

- Der Kartenleser liest das EF_CardAccess und extrahiert die für das PACE - Verfahren notwendigen Parameter
- Der Kartenleser extrahiert aus InputData die PIN – ID (PIN, CAN, MRZ, PUK) und sucht nach dem optional in den InputData enthaltenem CHAT um die Rolle des Terminals zu kontrollieren. Da es sich um ein Authentisierungsterminal handelt, wird das das PACE – Protokoll mit MST: Set AT eingeleitet:
  - MSE: Set AT
  - General Authenticate Step 1+2
- Der Kartenleser sucht in den InputData nach der optional enthaltenen 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 legt in der Variablen StoreHASH ab.
- Der Kartenleser fordert (sofern nicht in den InputData enthalten) zur PIN Eingabe auf und leitet danach Kπ ab. Gegebenenfalls kann der Kartenleser parallel zur Anzeige der Berechtigungen und der PIN - Eingabe bereits General Authenticate Step 2 und die Mappingfunktion durchführen.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

- Der Kartenleser entschlüsselt das ‚Encrypted Nonce' mit Kπ.
- Der Kartenleser bereinigt den Speicher von Informationen die Rückschlüsse auf die PIN zulassen.
- Der Kartenleser führt die restlichen Schritte General Authenticate Step 3+4 durch und bildet das Schlüsselmaterial für das SM.

A.10.2.2 Sichere Anzeige der eID-Informationen im Leserdisplay

- 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 StoreHASH gespeicherten Wert verglichen.
- Sind diese beiden Werte unterschiedlich, wird der Befehl geblockt und als Antwort SW1SW2 wird 69 85 zurückgegeben.

A.11 Mapping PACE Funktionen auf SCardControl

A.11.1 PC/SC-Mapping

Die in PC/SC 2.01.06 Part 10 spezifizierte Funktion ‚GET_FEATURE_REQUEST', wird erweitert:

```
#define FEATURE_EXECUTE_PACE   0x20
```

Der somit ermittelte Controlcode ‚CTRL_FEATURE_EXECUTE_PACE' wird dann mit SCardControl für alle PACE – Funktionen verwendet.

A.11.1.1 SCardControl

- InBuffer:

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

- Funktionsindizes:

Index	*Funktion*
1	GetReadersPACECapabilities
2	EstabishPACEChannel

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

- OutBuffer:

Position	*Länge in Bytes, Type*	*Name*	*Beschreibung*
1	4,DWORD	Result	Ergebniscode
2	2,WORD	lengthOutputData	Größe von Pos. 3
3	lengthOutputData	OutputData	Funktionsabhängige Ausgabedaten

- Ergebniscodes:

Code	*Beschreibung*
0x00000000	Kein Fehler
0xD0000001	Längen im Input sind inkonsistent
0xD0000002	Unerwartete Daten im Input
0xD0000003	Unerwartete Kombination von Daten im Input
0xE0000001	Die Karte unterstützt das PACE – Verfahren nicht. (Unerwartete Struktur in Antwortdaten der Karte)
0xE0000002	Der Kartenleser unterstützt den angeforderten bzw. den ermittelten Algorithmus nicht.
0xE0000003	Der Kartenleser kennt die PIN – ID nicht.
0xF000SW1SW2	Negative Antwort der Karte auf Select EF_CardAccess
0xF001SW1SW2	Negative Antwort der Karte auf Read Binary
0xF002SW1SW2	Negative Antwort der Karte auf MSE: Set AT
0xF003SW1SW2 – 0xF006SW1SW2	Negative Antwort der Karte auf General Authenticate Step 1-4
0xF0100001	Kommunikationsabbruch mit Karte.
0xF0100002	Keine Karte im Feld.
0xF0200001	Benutzerabbruch.
0xF0200002	Benutzer – Timeout

A.11.2 InputData und OutputData der einzelnen Funktionen

A.11.2.1 GetReadersPACECapabilities()

- InputData: Keine
- OutputData:

Position	*Länge in Bytes*	*Name*	*Beschreibung*
1	1	lengthBitMap	Größe von Pos. 2
2	lengthBitMap	BitMap	MSBit -> LSBit: PACE (0x40) EPA: eID (0x20)

			EPA: eSign (0x10)

A.11.2.2 EstablishPACEChannel(InputData)

- InputData:
  Positionen 2-7 sind optional vorhanden, wenn der Leser EPA: eID unterstützt.

Position	*Länge in Bytes*	*Name*	*Beschreibung*
1	1	PinID	0x01: MRZ 0x02: CAN 0x03: PIN 0x04: PUK
2	1	lengthCHAT	Größe von Pos. 3
3	lengthCHAT	CHAT	Das eingeschränkte CHAT für das Terminalzertifikat
4	1	lengthPIN	Größe von Pos.5
5	lengthPIN	PIN	PIN kann vom Host vorgegeben werden, z.B. gespeicherte CAN
6	2,WORD	lengthCertificateDescription	Größe von Pos. 9
7	lengthCertificateDescription	CertificateDescription	Komplette Zertifikatsbeschreibung, so, dass der Kartenleser den HASH berechnen kann.

- OutputData:

Position	*Länge in Bytes*	*Name*	*Beschreibung*
1	2	Statusbytes	Statusbytes bei Antwort auf MSE:SetAT
2	2,WORD	lengthEF_CardAccess	Größe von Pos. 3
3	lengthEF_CardAccess	EF_CardAccess	Gesamter Inhalt von EF_CardAccess
4	1	lengthCAR	Größe von Pos. 5
5	lengthCAR	CAR	Aktuelle Certificate Authority Reference
6	1	lengthCARprev	Größe von Pos. 7
7	lengthCARprev	CARprev	Vorangegangene Certificate Authority

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

			Reference
8	2,WORD	length_IDicc	Größe von Pos. 9
9	length_IDicc	IDicc	IDicc ist für spätere TA notwendig

Bemerkung: In der Rolle eines Signaturterminals entfallen Positionen Positionen 4-9, da automatisch der Terminaltunnel aufgebaut wird.

A.12 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 Seed mindestens 100 Bit beträgt.

A.13 Ansteuerung synchroner Chipkarten

Erkennt das CT beim Reset der Chipkarte eine synchrone Chipkarte so kann optional ein Modul für synchrone Chipkarten aktiviert werden.

Dieses Modul lässt die synchrone Chipkarte für die Applikationsschicht als Datei erscheinen. Dabei können durch das Auswählen unterschiedlicher Files zusätzliche Eigenschaften der Chipkarte angesprochen werden. Die Details zur Ansteuerung synchroner Chipkarten sind in Teil 7 der MKT Spezifikation beschrieben.

A.14 Bedienerschnittstellen

Chipkartenleser können über verschiedene Schnittstellen zum Bediener verfügen.

Neben Anzeigen über Leuchtdioden oder einem Textfeld (Display) sind auch Eingabeschnittstellen wie Tastatur oder biometrische Sensoren möglich.

Für den Fall, dass der Chipkartenleser diverse Bedienerschnittstellen aufweist, sind diese aus Interoperabilitätsgründen gemäß den nachfolgenden Beschreibungen auszuführen.

A.14.1 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 in einer zweiten Farbe (vorzugsweise gelb) angezeigt. Eine blinkende Leuchtdiode in der zweiten Farbe oder einer dritten Farbe signalisiert den Fehlerfall.

Mindestens eine Leuchtdioden-Anzeige muss 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. PC-Card Chipkartenleser) keine Möglichkeiten für eine Leuchtdiodenanzeige bieten.

A.14.2 Sicherheitsmodus Anzeige

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 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 und optische oder andere deutlich wahrzunehmenden Signale zur Verfügung zu stellen. Zusatzleuchten und Symbole in Displays sind derzeit gängige Anzeigen. Es sollte beachtet werden, dass eine behindertengerechte 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.

A.14.3 Display

Falls ein Display vorgesehen ist, ist die Größe von mindestens 2 Zeilen mit je mindestens 16 Zeichen zur Darstellung bereitzustellen.

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.

Für den oben beschriebenen Sicherheitsmodus sind Standardtexte im Chipkartenleser vorzuhalten. Folgende Standardtexte werden festgelegt:

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 9: Standard-Anzeigetexte

A.14.4 Tastatur

Der Chipkartenleser kann eine Tastatur besitzen. Falls eine Eingabetastatur vorhanden ist, sind folgende Regelungen zu beachten:

- Bei einer 12er-Tastatur sind die 11. und 12. Taste wie folgt vorzusehen:
  - Abbruchtaste und
  - Bestätigungstaste
- Wird eine 16er-Tastatur verwendet, sind außer den Zifferntasten die folgenden Tasten vorzusehen:
  - Abbruchtaste,
  - Korrekturtaste und
  - Bestätigungstaste

Auf eine ergonomisch günstige Ausprägung der Tastatur ist zu achten. Die Anordnung der Tasten kann in Anlehnung an CEN prEN 1332-5 [CEN1332] erfolgen.

Auch hier sollte auf eine behindertengerechte Ausführung, z. B. durch ein fühlbares Tastenfeld oder durch Brailleschrift, geachtet werden.

A.14.5 Biometrischer Sensor

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

Die biometrischen Daten gelangen dazu nicht in die unsichere Umgebung des Hosts.

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

Die Bewertung für die Einsatzfähigkeit in abgegrenzter Anwendung und definierter Umgebung erfolgt durch eine separate Untersuchung und ist nicht Gegenstand der Prüfungen zum Erhalt des Prüfzeugnisses. Zusatzprüfungen können aber im Prüfzeugnis mit aufgenommen werden.

A.14.6 Weitere Schnittstellen

Jede andere geeignete Schnittstelle zum Bediener kann optional in einem Chipkartenleser eingesetzt werden. Dabei ist darauf zu achten, dass sie weder in Funktion noch im Sicherheitslevel die zuvor definierten Schnittstellen beeinträchtigt. Weitere Schnittstellen werden in den Standardprüfungen zum Prüfungszeugnis nicht berücksichtigt und können durch eine freiwillige und individuelle Prüfung mit aufgenommen werden.

A.15 Stromversorgung

Die externe Stromversorgung des Chipkartenlesers muss so beschaffen sein, dass ein Dauerbetrieb des Chipkartenlesers von 24 Stunden pro Tag möglich ist, ohne dass eine Einschränkung der Funktionsfähigkeit zu verzeichnen ist.

Dies schließt mit ein, dass eine dauerhafte Stromversorgung der Chipkarte mit dem Maximalstrom nach ISO/IEC 7816-3 gewährleisten sein muss. Dabei ist zu beachten, dass Chipkarten kurzzeitig auch einen höheren Strombedarf haben können. In jedem Fall muss auch hier die volle Funktionsfähigkeit des Chipkartenlesers gewährleistet sein.

Ebenso ist hierbei die Stromaufnahme der kontaktlosen Chipkarte zu berücksichtigen.

A.16 Firmwareupdate

Werden Chipkartenleser gefordert, bei denen Leistungsanpassungen auf Grund veränderter Umgebungsbedingungen notwendig werden können, müssen die Chipkartenleser mit einer Secure-Download-Funktion ausgestattet sein. Diese Firmware des Chipkartenlesers ist elementare Grundlage für die Sicherstellung der geprüften Leitungsmerkmale. Daher ist der Download-Vorgang so abzusichern, dass die Chipkarten-Firmware nicht unbefugt verändern kann.

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

Mit einem kryptographischen Sicherungssystem wird sichergestellt, 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 kann eine Absicherung über eine Verschlüsselung oder über eine digitale Signatur der Daten erfolgen. Die spätere Anwendung bestimmt die Höhe des Sicherheitslevels an dieser Stelle.

A.17 Verfügbarkeit

Bei Ausfall von Hardwarekomponenten darf der Chipkartenleser nicht in einen undefinierten Zustand schalten, sondern mit Abbruch und / oder Fehlermeldungen reagieren.

Bei einer Inbetriebnahme oder Reset wird eine automatische Initialisierung des Chipkartenlesers vorgenommen. Es wird auf die Standardeinstellungen für die Kommunikation mit dem Host zurückgeschaltet. Der Endbenutzer muss erkennen können, dass das Gerät nicht manipuliert wurde. Es ist zusätzlich der Auslieferungszustand und das Auslieferungsverfahren zu beschreiben.

A.18 Vertraulichkeit und Integrität

Die PIN / das Passwort gelangen durch bauliche Maßnahmen (z. B.: Tastatur im Leser), nicht in die Umgebung des Hosts, sondern werden ohne Umwege im Chipkartenleser verarbeitet und direkt an die Karte weitergegeben (Secure Mode).

Wird das Display mit Standardtexten angesteuert, so ist dieses zu signalisieren (Secure Mode).

Die PIN / das Passwort darf nicht auf der Luftschnittstelle im Klartext übermittelt werden (s. PACE).

Die Chipkarte und deren Applikationen dürfen nicht unbemerkt aktiviert und unbemerkt benutzt werden. Es muss stets eine gesonderte Willenserklärung des Nutzers möglich oder explizit die akute Nutzung durch geeignete Anzeigen erkennbar sein.

Ein Betrieb im sicheren Modus (Secure Mode) wird unzweifelhaft signalisiert und darf nicht von außen steuerbar sein. Der Benutzer ist über die Dokumentation eindeutig über den sicheren Modus zu informieren.

A.19 Sichere PIN Eingabe

Die PIN wird direkt über die Tastatur des Terminals bzw. des Lesers an die Chipkarte übertragen, die Daten verlassen nicht das Terminal. Die Verifikation der PIN findet auf der Karte statt.

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

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

B Prüfanforderungen

B.1 Umweltanforderungen

Die Einsatzumgebungen der nachfolgenden Anforderungen sind für allgemeine Industrieanwendungen, Büros, öffentliche Gebäude, Fertigungsstätten für elektronische und andere elektronische Erzeugnisse, Fabrikationsräume für Großbetriebe, Lagerräume, Wohn- und Arbeitsbereiche ausgelegt.

Angenommen wird ein ortsfester, wettergeschützter Einsatzort ohne Temperaturregelung. Wenn notwendig kann zur Vermeidung extrem niedriger Temperaturen geheizt werden. Betauung ist ebenfalls möglich.

An diesen Einsatzorten können auch merkliche Schwingungen und Stöße auftreten, hervorgerufen z. B. von Maschinen oder in der Nähe vorbeifahrender Fahrzeuge.

Chipkartenleser im Freien, kaum oder nicht wettergeschützte Chipkartenleser oder bei Betrieb an Einsatzorte mit einem sehr hohen Schwingungspegel, bedürfen gesonderter Betrachtung.

B.1.1 CE-Kennzeichnung

Es ist eine schriftliche Herstellererklärung gemäß den Anforderungen zur CE-Kennzeichnung erforderlich. Der Hersteller bestätigt die Konformität des Produktes mit den Inverkehrbringungs- und Entsorgungs- Richtlinien der EU und die Einhaltung der darin festgelegten Anforderungen und Grenzwerte.

B.1.2 Klima

Die durch Klimaschwankungen auftretenden Belastungen müssen vom Chipkartenleser schadensfrei absolviert werden und werden durch Herstellererklärung unter Offenlegung der zugrunde gelegten Anforderungen bzw. Prüfverfahren nachgewiesen.

B.1.3 Vibration

Die durch Vibrationen und mechanische Schockbelastungen auftretenden Belastungen müssen vom Chipkartenleser schadensfrei absolviert werden und werden durch Herstellererklärung unter Offenlegung der zugrunde gelegten Anforderungen bzw. Prüfverfahren nachgewiesen.

B.2 Konformitätsanforderungen

Für alle in dieser TR beschriebenen Lesertypen sind Konformitätstests der ISO Layer 2-4 nach TR-03105 Teil 4 bei den dafür legitimierten Stellen durchzuführen.

Zur Validierung der PACE Implementierung sind zusätzlich für Standard- sowie Komfort-Chipkartenleser die relevanten Teile von ISO Layer 6-7 nach TR-03105 Teil 5.2 prüfen zu lassen.

Zur Validierung der EAC/QES Implementierung sind zusätzlich für Standard-Chipkartenleser mit ePA-QES sowie Komfort-Chipkartenleser die relevanten Teile von ISO Layer 6-7 nach TR-03105 Teil 5.2 prüfen zu lassen.

B.2.1 Funktionale Prüfung

Die Funktionsprüfung stellt die Interoperabilität zwischen verschiedenen Chipkartenlesern sicher und testet Grundlagenanforderungen durch eine praktische Prüfung.

Mittels Referenzimplementierung (Bürgerclient) und technischen Daten werden getestet:

- Unterstützung verschiedener Betriebssysteme
  - hier: aktuelle Versionen des Heimbereichs (siehe A.9)
- Installation des ePA Cat-B Chipkartenlesers

B.3 Sicherheitsanforderungen

Je nach Einsatzgebiet und Ausprägung des Chipkartenlesers können **Evaluierungen/ Zertifizierungen** nach den „Common Criteria for Information Technology Security Evaluation V 3.1 (CC)“ erforderlich sein.

Beispielsweise verlangen Anwendungen gemäß des deutschen Signaturgesetzes (SigG) mindestens EAL3+ Evaluierungen.

Für diverse Einsätze im Bankenumfeld sind Gutachten und Zulassungen des Zentralen Kreditausschusses (ZKA) notwendig.

Die Zertifizierung, SigG Bestätigung oder ein ZKA-Gutachten ist bei den dafür legitimierten Stellen durchzuführen.

Als Mindestanforderung für Chipkartenleser der Kategorien Cat-S und Cat-K ist ein **Sicherheitsgutachten** notwendig.

Dazu werden folgende Aspekte begutachtet:

- **Vertraulichkeit**
- **Integrität und**
- **Verfügbarkeit**

Zusätzliche oder neue Anforderungen, die sich aus einer speziellen Anwendung oder durch neue bzw. aktuelle Sicherheitsbetrachtungen ergeben, können mit in das Sicherheitsgutachten aufgenommen werden.

Diese werden dann als eine erweiterte Anforderung in den Umfang der gesamten Abnahmeprozedur (Validierung) eingebunden oder werden in einer Nachvalidierung nachträglich geleistet.

An dieser Stelle werden keine speziellen Vorgaben gemacht. Die individuellen Ausprägungen (Bauform, PIN, Biometrie, Anzeigen usw.) bestimmen den Prüfaufwand.

Gemäß den oben genannten Aspekten der Informationssicherheit wird definierten Bedrohungen entgegengewirkt und definierten Sicherheitszielen entsprochen.

B.4 Spezielle SigG Anforderungen für den ePA

Sollen qualifizierte Signaturen durchgeführt werden, ist die Komponente (Chipkartenleser) gemäß den konkretisierten Anforderungen der Signaturverordnung (Verordnung zur elektronischen Signatur (Signaturverordnung – SigV)) zu evaluieren und von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) oder einer akkreditierten Bestätigungsstelle zu bestätigen.

Zur Erzeugung qualifizierter Signaturen werden – neben einer sicheren Signaturerstellungseinheit (SSEE) – sowohl ein Kartenlesegerät als auch entsprechende Software (zusammen SAK – Signaturanwendungskomponente) benötigt. Während die Verwendung einer SSEE darüber sichergestellt wird, dass private Schlüssel für qualifizierte Signaturen vom ZDA ausschließlich auf solchen SSEE verteilt bzw. erzeugt werden, kann die Verwendung einer sicheren Kartenlesers bzw. sicherer Software in der Regel nicht technisch erzwungen werden.

Über den Mechanismus der Terminalauthentisierung des elektronischen Personalausweises bietet sich nun die Möglichkeit, zumindest für den Kartenleser zu erzwingen, dass nur bestätigte Leser zur Erstellung qualifizierter Signaturen verwendet werden können.

Im Folgenden wird der Ablauf der Authentisierung eines Kartenlesers als Signaturterminal gegenüber dem Personalausweis in Vorbereitung auf eine Signaturerstellung betrachtet. Das Erzeugen eines qualifizierten Schlüsselpaares bzw. Nachladen eines qualifizierten Zertifikates erfolgt in der Rolle eines Authentisierungsterminals und ist somit nicht Gegenstand dieser Darstellung.

Die Authentisierung eines Kartenlesers gegenüber dem Ausweis erfolgt durch mehrere aufeinander folgende kryptographische Protokolle. Der genaue Ablauf wird in [TR-03110] und [TR-03117] beschrieben.

B.4.1 PACE

Dieses Protokoll dient dem Aufbau eines sicheren Kanals (Secure Messaging) zwischen Kartenleser und Ausweis. Der Aufbau des Kanals gelingt nur, wenn als Eingabeparameter für das Protokoll das korrekte Passwort genutzt wurde. Im Falle eines Signaturterminals ist dies die Kartenzugangsnummer (CAN). 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).

B.4.2 Terminalauthentisierung

Über die Terminalauthentisierung weist sich der Leser als bestätigtes Signaturterminal aus. Über diesen Mechanismus kann der Ausweis den Einsatz in einer für die QES geeigneten Umgebung zumindest zum Teil überprüfen, somit wird das Sicherheitsniveau der QES-Erzeugung deutlich angehoben.

Zur Durchführung der Terminalauthentisierung muss der Leser einen privaten Schlüssel besitzen und mit diesem eine Signatur erzeugen können. Der zugehörige öffentliche Schlüssel muss von einer durch die Wurzelinstanz der EAC-PKI (BSI) zertifizierten Stelle (DV) für die Rolle „Signaturterminal für qualifizierte Signaturen“ zertifiziert werden.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

B.4.3 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. 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.

B.4.4 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.

B.4.5 PIN-Verifikation und Signaturauslösung

Die Verifikation der Signatur-PIN und die Erzeugung der Signatur erfolgt mit Standard-Kommandos nach ISO 7816, wie in [TR-03117] beschrieben und stellt keine neuen Anforderungen an den Kartenleser.

B.4.6 Terminalzertifikat

Die Zertifizierung der Leser 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 (jeweils auf hohem Sicherheitsniveau) ist Bestandteil der Evaluierung im Rahmen der Bestätigung. Nach erfolgter Bestätigung des Lesertyps wird der öffentliche Schlüssel durch das BSI zertifiziert.

Zur Bindung des Zertifikates an eine bestätigte Firmware ist der Hashwert der Firmware Bestandteil des Zertifikates. Dadurch kann die Software, die für ein Firmware-Update des Lesers genutzt wird, die Zusammengehörigkeit von Firmware und Zertifikat überprüfen.

Zur Rezertifizierung stellt der Hersteller einen neuen Zertifizierungsantrag 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.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

B.4.7 Anforderungen an den Kartenleser

Aus dem dargestellten Ablauf leiten sich folgende – gegenüber vorhandenen Signaturkartenlesern – neuen Anforderungen an den Kartenleser ab:

1. Der Kartenleser beherrscht Secure Messaging, PACE, Terminalauthentisierung, Passive Authentisierung und Chipauthentisierung.
2. Für die Terminalauthentisierung muss das Terminal einen privaten Schlüssel sicher speichern. Der Schlüssel muss in einem nach CC EAL4+ zertifizierten Modul gespeichert werden, welches die für die Terminalauthentisierung benötigte Signatur erzeugen kann. Denkbar ist hier z.B. ein nach [PP-SSCD] zertifizierter Chip. Die auf den Chip zugreifende Software (Firmware) muss nach 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.
3. Optional: Sofern der Import eines neuen privaten Schlüssels möglich sein soll, so muss dieser Import entsprechend abgesichert werden. Der Import muss nach CC EAL4+ zertifiziert werden. Dies wird nicht durch [PP-IS] abgedeckt, muss also im Security Target zusätzlich berücksichtigt werden.
4. Für die Erneuerung des Terminalzertifikates muss der Import des Zertifikates und der zugehörigen Zertifikatskette in den Leser möglich sein. Denkbar ist hier die Nutzung eines vorhandenen Mechanismus zum Firmware-Update.
5. Für die Passive Authentisierung muss das Terminal in der Lage sein, das CSCA-Zertifikat manipulationssicher zu speichern. Die sichere Speicherung ist durch [PP-IS] abgedeckt.

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Referenzen

[ISO1] ISO/IEC 7810: 2003, Identification cards – Physical characteristics

[ISO2] ISO/IEC 7816-2: 1999, Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts

[ISO3] ISO/IEC 7816-3: 2006, Identification cards – Integrated circuit(s) cards – cards with contacts – Part 3: Electrical interface and transmission protocols

[ISO4] ISO/IEC 7816-4: 2005, Identification cards – Integrated circuit(s) cards with contacts – Part 4: Organization, security and commands for interchange

[ISO10] ISO/IEC 7816-10:1999, Identification cards – Integrated circuit(s) cards with contacts – Part 10: Electronic signals and answer to reset for synchronous cards

[PICC1] ISO/IEC 14443-1: 2001, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical Characteristics

[PICC2] ISO/IEC 14443-2: 2001, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio Frequency power and signal interface

[PICC3] ISO/IEC 14443-3: 2001, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and Anticollision

[PICC4] ISO/IEC 14443-4: 2001, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission Protocol

[CT-API] Teletrust, CT-API – Anwendungsunabhängiges CardTerminal Application Programming Interface für Chipkartenanwendungen,
http://www.ct-api.de

[PC/SC] PC/SC Workgroup:
PC/SC Workgroup Specifications 1.0/2.0,
http://pcscworkgroup.com

[SICCT] TeleTrusT, Secure Interoperable ChipCard Terminal (SICCT),
http://www2.teletrust.de/fileadmin/files/publikationen/Spezifikationen/SICCT_Spezifikation_120.pdf

[PP-IS] BSI: Common Criteria Protection Profile for Inspection Systems, BSI-CC-PP-0064

[PP-SSCD] CEN: Protection Profile Secure Signature Creation DeviceType 3, BSI-CC-PP-00xx

[TR-03105] BSI: Technische Richtlinie TR-03105, Conformity Tests for Official Electronic ID Documents

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger

Part 4: „Test plan for ICAO compliant Proximity Coupling Device (PCD) on Layer 2-4“

Part 5.2: „Test plan for eID-Card compliant Reader Systems with EAC 2.0“

[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

[MKT] TeleTrust, Multifunktionale KartenTerminals MKT-Spezifikation – MKT-Version 1.0

[EMV2000] EMV, Integrated Circuit Card, Specification for Payment Systems, Application Independent ICC to Terminal Interface Requirements

[CEN1375] CEN ENV 1375-1: 1994, Identification card systems – Intersector integrated circuit(s) card additional formats – Part 1: ID-000 card size and physical characteristics

[CEN1332] CEN prEN 1332-5: 1995, Identification card systems – Man machine interface – Part 5: Raised tactile symbols for differentiation of application on ID-1 cards

Nichtamtlicher Hinweis der Bundesanzeiger Verlagsges.mbH:
Auftraggeber der Veröffentlichung:
Bundesamt für Sicherheit in der Informationstechnik
Erlassdatum: 15. Oktober 2010
Fundstelle: eBAnz AT114 2010 B1
– veröffentlicht am 29. Oktober 2010 –
Quelle: elektronischer Bundesanzeiger